BUKU PEGANGAN TANGGAP INSIDEN SIBER

HANDBOOK OF CYBER INCIDENT RESPONSE

Oleh : Restia Moegiono {CEH|CHFI|ECSA|QRMO}

Riwayat Perubahan

Versi	Tanggal	Personel	Perubahan
0.0	1 Maret 2023	Restia Moegiono	Versi awal Buku Pegangan Tanggap Insiden Siber

Daftar Isi

Riwayat Perubahan .... *i*

Daftar Isi .... *ii*

1 - Tanggap Insiden (Incident Response) *1*

a. Pentingnya Tanggap Insiden 1

b. Siklus Tanggap Insiden (*Incident Response Life Cycle*) 1

2 - Tim Tanggap Insiden Siber *5*

a. Tugas Tim Tanggap Insiden Siber Organisasi 5

b. Layanan Tim Tanggap Insiden Siber 5

c. Sub Tim Dalam Tim Tanggap Insiden Siber 11

d. Model Tim Tanggap Insiden Siber 12

e. Sumber Daya Tim Tanggap Insiden Siber 12

f. Perangkat Pendukung Tim Tanggap Insiden Siber 29

3 - Malware Jenis Worm *31*

a. Persiapan 31

b. Identifikasi 31

c. Penahanan (*Containment*) 32

d. Perbaikan (*Remediation*) 32

e. Pemulihan (*Recovery*) 33

f. Pelajaran yang Diperoleh (*Lesson Learned*) 33

4 - Intrusi pada Windows *34*

a. Persiapan 34

b. Identifikasi 35

c. Penahanan (*Containment*) 36

d. Perbaikan (*Remediation*) 37

e. Pemulihan (*Recovery*) 38

f. Pelajaran yang Diperoleh (*Lesson Learned*) 38

5 - Intrusi pada Unix/Linux 39

a. Persiapan 39

b. Identifikasi 39

c. Penahanan (*Containment*) 42

d. Perbaikan (*Remediation*) 43

e. Pemulihan (*Recovery*) 43

f. Pelajaran yang Diperoleh (*Lesson Learned*) 43

6 - DDoS 45

a. Persiapan 45

b. Identifikasi 46

c. Penahanan (*Containment*) 47

d. Perbaikan (*Remediation*) 48

e. Pemulihan (*Recovery*) 48

f. Pelajaran yang Diperoleh (*Lesson Learned*) 49

7 - Perilaku Jaringan Berbahaya (Malicious Network Behaviour) 50

a. Persiapan 50

b. Identifikasi 50

c. Penahanan (*Containment*) 51

d. Perbaikan (*Remediation*) 52

e. Pemulihan (*Recovery*) 53

f. Pelajaran yang Diperoleh (*Lesson Learned*) 53

8 - Website Defacement 54

a. Persiapan 54

12 - Social Engineering *70*

a. **Persiapan** **70**

b. **Identifikasi** **70**

c. **Penahanan (*Containment*)** **71**

d. **Perbaikan (*Remediation*)** **73**

e. **Pemulihan (*Recovery*)** **73**

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** **73**

13 - Kebocoran Informasi (Information Leakage) *74*

a. **Persiapan** **74**

b. **Identifikasi** **74**

c. **Penahanan (*Containment*)** **76**

d. **Perbaikan (*Remediation*)** **77**

e. **Pemulihan (*Recovery*)** **77**

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** **78**

14 - Penyalahgunaan Orang Dalam (Insider Abuse) *79*

a. **Persiapan** **79**

b. **Identifikasi** **79**

c. **Penahanan (*Containment*)** **80**

d. **Perbaikan (*Remediation*)** **81**

e. **Pemulihan (*Recovery*)** **82**

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** **82**

15 - Phishing pada Pelanggan *83*

a. **Persiapan** **83**

b. **Identifikasi** **84**

c. **Penahanan (*Containment*)** **85**

d. **Perbaikan (*Remediation*)** **85**

e. **Pemulihan (*Recovery*)** 86

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** 86

16 - Penipuan (Scam) *88*

a. **Persiapan** 88

b. **Identifikasi** 89

c. **Penahanan (*Containment*)** 90

d. **Perbaikan (*Containment*)** 90

e. **Pemulihan (*Recovery*)** 91

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** 91

17 - Pelanggaran Merek Dagang *92*

a. **Persiapan** 92

b. **Identifikasi** 93

c. **Penahanan (*Containment*)** 93

d. **Perbaikan (*Remediation*)** 94

e. **Pemulihan (*Recovery*)** 94

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** 95

18 - Phishing *96*

a. **Persiapan** 96

b. **Identifikasi** 97

c. **Penahanan (*Containment*)** 98

d. **Perbaikan (*Remediation*)** 98

e. **Pemulihan (*Recovery*)** 98

f. **Pelajaran yang Diperoleh (*Lesson Learned*)** 99

19 - Ransomware *100*

a. **Persiapan** 100

b. **Penahanan (*Containment*)** 101

c. Perbaikan (*Remediation*) 102

d. Pemulihan (*Recovery*) 102

e. Pelajaran yang Diperoleh (*Lesson Learned*) 102

20 - Penyusupan/Kompromi Skala Besar 104

a. Persiapan 104

b. Identifikasi 105

c. Penahanan (*Containment*) 106

d. Perbaikan (*Remediation*) 107

e. Pemulihan (*Recovery*) 108

f. Pelajaran yang Diperoleh (*Lesson Learned*) 109

Kosakata 110

Referensi 111

1 - Tanggap Insiden (*Incident Response*)

a. Pentingnya Tanggap Insiden

Tanggap inisiden merupakan serangkaian komponen atas *people, process, technology* pada keamanan informasi yang digunakan untuk mengidentifikasi, menahan, dan menghilangkan insiden siber. Tujuan dari tanggap insiden adalah untuk memungkinkan organisasi mendeteksi dan menghentikan insiden dengan cepat, meminimalkan kerusakan, dan mencegah ternjadinya insiden jenis yang sama di masa mendatang.

1) Pada aspek *people*

   Diperlukan Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*) yang menjalankan fungsi tanggap insiden di tingkat organisasi untuk menanggapi insiden siber dengan cepat, efektif dan efisien, sehingga dapat meminimalkan dampak kerusakan dan melindungi kepentingan umum.

2) Pada aspek *process*

   Diperlukan kebijakan, prosedur, dan dokumentasi yang mendukung tanggap insiden.

3) Pada aspek *technology*

   Diperlukan penerapan teknologi yang mendukung operasi tanggap insiden.

b. Siklus Tanggap Insiden (*Incident Response Life Cycle*)

1) Persiapan

Persiapan pada siklus tanggap insiden sangat penting karena tidak hanya menetapkan kemampuan tanggap insiden, tetapi juga mencegah insiden dengan memastikan bahwa sistem, jaringan, dan aplikasi dalam keadaan yang cukup aman. Meskipun Tim Tanggap Insiden Siber biasanya tidak bertanggung jawab untuk pencegahan insiden, namun tahap hal ini sangat penting untuk keberhasilan program tanggap insiden. Tahap ini berisikan persiapan untuk menangani insiden dan pencegahan insiden.

2) **Identifikasi**

Tim Tanggap Insiden Siber harus bekerja dengan cepat untuk menganalisis dan memvalidasi setiap insiden, mengikuti proses yang telah ditentukan sebelumnya dan mendokumentasikan setiap langkah yang diambil. Saat Tim Tanggap Insiden Siber yakin bahwa insiden telah terjadi, maka Tim Tanggap Insiden Siber harus segera melakukan analisis awal untuk menentukan cakupan insiden, seperti jaringan, sistem, atau aplikasi mana yang terpengaruh; siapa atau apa yang memulai insiden itu; dan bagaimana insiden tersebut terjadi (misalnya, alat atau metode serangan apa yang digunakan, kerentanan apa yang dieksploitasi). Analisis awal harus memberikan informasi yang cukup bagi Tim Tanggap Insiden Siber untuk memprioritaskan aktivitas selanjutnya, seperti penahanan insiden dan analisis yang lebih dalam tentang dampak insiden.

Tim Tanggap Insiden Siber yang mencurigai adanya insiden harus segera mulai mencatat semua fakta terkait insiden tersebut. Mendokumentasikan kejadian, percakapan, dan perubahan yang diamati dalam *file* dapat mengarah pada penanganan masalah yang lebih efisien, lebih sistematis, dan dapat meminimalisir kesalahan. Setiap langkah yang diambil sejak insiden terdeteksi hingga penyelesaian akhirnya harus didokumentasikan dan diberi *timestamp*. Setiap dokumen mengenai insiden harus diberi tanggal dan ditandatangani oleh anggota TIm Tanggap Insiden Siber. Informasi semacam ini juga dapat digunakan sebagai bukti di pengadilan jika tuntutan hukum dilakukan.

Ketika sebuah insiden dianalisis dan diprioritaskan, Tim Tanggap Insiden Siber perlu memberi tahu individu yang tepat sehingga semua yang perlu terlibat akan menjalankan perannya masing-masing. Kebijakan tanggap insiden harus mencakup ketentuan tentang pelaporan insiden seperti, apa yang harus dilaporkan kepada siapa dan kapan (pemberitahuan awal, pembaruan status pada penanganan insiden). Persyaratan pelaporan dapat bervariasi pada berbagai organisasi.

3) **Penahanan (*Containment*)**

Penahanan penting sebelum insiden mempengaruhi sumber daya atau meningkatkan kerusakan. Penahanan menyediakan waktu untuk mengembangkan strategi perbaikan yang relevan. Bagian penting dari penahanan adalah pengambilan keputusan dan hal ini jauh lebih mudah dibuat jika ada strategi dan prosedur yang telah ditentukan sebelumnya untuk mengatasi insiden tersebut. Organisasi harus mendefinisikan risiko yang dapat diterima dalam menghadapi insiden dan mengembangkan strategi yang sesuai.

Strategi penahanan bervariasi berdasarkan jenis insiden. Organisasi harus membuat strategi penahanan terpisah untuk setiap jenis insiden besar, dengan kriteria yang

didokumentasikan dengan jelas untuk memfasilitasi pengambilan keputusan. Kriteria penentuan strategi yang tepat mempertimbangkan hal-hal berikut:

- Potensi kerusakan dan pencurian sumber daya.
- Kebutuhan untuk menyimpan bukti (*evidence*).
- Ketersediaan layanan.
- Waktu dan sumber daya yang dibutuhkan untuk menerapkan strategi penahanan.
- Keefektifan strategi, misalnya penahanan sebagian, penahanan penuh.
- Durasi solusi yang diterapkan, misalnya solusi darurat akan dihapus dalam 4 (empat) jam, solusi sementara akan dihapus dalam 2 (dua) minggu, dan solusi permanen.

4) Perbaikan (*Remediation*)

Setelah Tim Tanggap Insiden Siber melakukan penahanan, perencanaan perbaikan dilakukan dengan:

- Penghapusan ancaman

  Tim Tanggap Insiden Siber menghapus persistensi peretas, memblokir hak akses peretas, dan menutup semua vektor/sumber serangan.
- Perbaikan kontrol keamanan

  Kontrol keamanan diperbarui dengan menghapus kerentanan untuk mencegah insiden serupa di masa mendatang. Perbaikan ini dilakukan dengan melakukan *update*, memasang *patch*, atau penggantian *password* untuk memastikan lingkungan aman. Proses dan *tools* baru dapat diterapkan untuk memperketat perimeter keamanan di jaringan internal, *host* internal, aplikasi, dan data. *Level logging pada* sistem atau pemantauan jaringan juga perlu dibuat yang lebih tinggi/detail. Hal ini penting untuk diperhatikan karena setelah sumber daya berhasil diserang, sering kali diserang lagi, atau sumber daya lain dalam organisasi diserang dengan cara yang sama. Pada tahap ini pastikan setiap tindakan didokumentasikan, seperti apa yang terjadi dan tindakan perbaikannya.

5) Pemulihan (*Recovery*)

Dalam pemulihan dilakukan tindakan untuk mengembalikan sistem ke operasi normal dan mengonfirmasi bahwa sistem berfungsi normal. Pemulihan mungkin melibatkan tindakan seperti memulihkan sistem dari *backup* yang bersih, membangun kembali sistem dari awal, dan mengganti *file* yang disusupi dengan *file* yang versi bersih. Pada insiden skala besar, tahap perbaikan dan pemulihan bisa memakan waktu berbulan-bulan karena dilakukan meningkatkan keamanan secara keseluruhan untuk mencegah insiden di masa mendatang dan fokus pada perubahan jangka panjang dan berkelanjutan untuk menjaga agar organisasi seaman mungkin.

6) **Pelajaran yang Diperoleh (*Lesson Learned*)**

Salah satu bagian terpenting dari tanggap insiden juga yang paling sering diabaikan, yaitu mendapatkan pembelajaran dan melakukan peningkatan. Setiap Tim Tanggap Insiden Siber harus melakukan perubahan berdasarkan adanya ancaman baru, peningkatan teknologi, dan pembelajaran yang diperoleh.

Organisasi perlu mengadakan pertemuan dalam beberapa hari setelah insiden siber berakhir, untuk membahas pembelajaran yang diperoleh dengan semua pihak yang terlibat setelah terjadi insiden berskala besar, dan secara opsional setelah insiden yang lebih kecil. Pembelajaran ini dapat sangat membantu dalam meningkatkan tindakan keamanan dan proses penanganan insiden itu sendiri. Pertemuan ini memberikan kesempatan untuk melakukan evaluasi penanganan insiden dengan meninjau apa yang terjadi, apa yang sudah dilakukan, dan seberapa baik prosedur penanganan insiden siber bekerja. Pertanyaan yang akan dijawab dalam pertemuan tersebut antara lain:

- Tepatnya apa yang terjadi, dan pada waktu apa?
- Seberapa baik kinerja staf dan manajemen dalam menangani insiden tersebut?
- Apakah prosedur terdokumentasi diikuti? Apakah prosedur tersebut sudah memadai?
- Informasi apa yang dibutuhkan lebih awal?
- Apakah ada langkah atau tindakan yang diambil yang mungkin menghambat pemulihan?
- Apa yang akan dilakukan oleh staf dan manajemen secara berbeda saat insiden serupa terjadi lagi?
- Bagaimana berbagi informasi dengan organisasi lain dapat ditingkatkan?
- Tindakan korektif apa yang dapat mencegah kejadian serupa di masa depan?
- Indikator apa yang harus diperhatikan di masa depan untuk mendeteksi insiden serupa?
- *Tools* atau sumber daya tambahan apa yang diperlukan untuk mendeteksi, menganalisis, dan mengurangi insiden di masa mendatang?

Kegiatan pasca-insiden penting lainnya adalah membuat laporan penanganan insiden yang sangat berharga untuk digunakan di masa mendatang. Laporan tersebut memberikan referensi yang dapat digunakan untuk membantu penanganan insiden serupa. Membuat kronologi kejadian yang formal penting untuk mendukung aspek hukum, seperti halnya membuat perkiraan dampak finansial atas kerusakan yang disebabkan oleh insiden tersebut.

2 - Tim Tanggap Insiden Siber

a. Tugas Tim Tanggap Insiden Siber Organisasi

Sesuai dengan Peraturan BSSN Nomor 10 Tahun 2020, Tim Tanggap Insiden Siber (*Computer Security Incident Response Team* - CSIRT) adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya. Tim Tanggap Insiden Siber yang menangani insiden siber di organisasi memiliki tugas, antara lain:

1) Menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan insiden siber di organisasinya.
2) Mengoordinasikan penanganan insiden siber tingkat organisasi.
3) Merumuskan panduan teknis penanganan insiden siber tingkat organisasi.
4) Melakukan koordinasi dengan Tim Tanggap Insiden Siber Sektoral atau dengan Tim Tanggap Insiden Siber Nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber Sektoral.
5) Memberikan bantuan yang diperlukan bagi konstituen.
6) Memberikan laporan penanganan insiden siber yang telah terjadi kepada pimpinan organisasi dan Tim Tanggap Insiden Siber Sektoral atau Tim Tanggap Insiden Siber Nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber Sektoral.
7) Melakukan koordinasi dan/atau kerja sama dengan pihak lain dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

b. Layanan Tim Tanggap Insiden Siber

Layanan yang diberikan oleh Tim Tanggap Insiden Siber bergantung kepada jenis dari Tim Tanggap Insiden Siber, tingkat kematangan (*maturity*) dari Tim Tanggap Insiden Siber, dan sumber daya yang dimiliki. Jenis dan kedalaman (*depth*) dari layanan Tim Tanggap Insiden Siber juga dapat bervariasi. Layanan Tim Tanggap Insiden Siber dalam perspektif ketersediaan sumber daya, terdiri atas :

1) Layanan Utama

   Layanan utama merupakan layanan yang harus ditetapkan dan diberikan oleh Tim Tanggap Insiden Siber kepada konstituen.

2) Layanan Tambahan

   Layanan tambahan merupakan layanan ditetapkan dan diberikan oleh Tim Tanggap Insiden Siber sesuai dengan kebutuhan konstituen dan ketersediaan sumber daya Tim Tanggap Insiden Siber.

Berikut adalah beberapa layanan yang dapat disediakan Tim Tanggap Insiden Siber.

	Sifat Layanan		
	Layanan Reaktif	Layanan Proaktif	Layanan Peningkatan Kesiapan Penanganan Insiden Siber
Layanan Utama	1. Pemberian peringatan terkait keamanan siber 2. Penanganan insiden siber		
Layanan Tambahan	1. Penanganan kerawanan sistem elektronik 2. Penanganan artefak digital	3. Pemberitahuan hasil pengamatan potensi ancaman 4. Pendeteksian serangan	5. Analisis risiko keamanan siber 6. Konsultasi terkait kesiapan penanganan Insiden Siber 7. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Adapun layanan Tim Tanggap Insiden Siber dalam perspektif sifat layanan, yaitu :

1) Layanan Reaktif

   Layanan ini dipicu oleh suatu peristiwa atau permintaan, seperti laporan *host* yang diretas, *malicious code* yang menyebar luas, kerentanan perangkat lunak, atau sesuatu yang diidentifikasi oleh perangkat deteksi intrusi atau sistem *logging*. Layanan reaktif adalah komponen inti dari pekerjaan Tim Tanggap Insiden Siber.

2) Layanan Proaktif

   Layanan ini memberikan bantuan dan informasi untuk mempersiapkan, melindungi, dan mengamankan sistem elektronik untuk mengantisipasi serangan, masalah, atau peristiwa. Kinerja layanan ini secara langsung akan mengurangi jumlah insiden di masa depan.

3) Layanan Peningkatan Kesiapan Penanganan Insiden Siber

   Layanan ini menambah layanan yang independen dari penanganan insiden dan dilakukan oleh area lain dari organisasi seperti unit kerja yang membawahi fungsi IT, audit, atau pelatihan. Jika suatu Tim Tanggap Insiden Siber melakukan atau membantu dengan layanan ini, sudut pandang dan keahlian Tim Tanggap Insiden Siber dapat memberikan wawasan untuk membantu meningkatkan keamanan keseluruhan organisasi dan mengidentifikasi risiko, ancaman, dan kelemahan sistem. Layanan ini umumnya proaktif tetapi berkontribusi secara tidak langsung untuk mengurangi jumlah insiden.

Penjelasan untuk layanan utama Tim Tanggap Insiden Siber yaitu :

1) Pemberian peringatan terkait keamanan siber (*alert and warning*)

   Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk menyebarluaskan informasi kepada konstituen terkait keamanan siber, seperti serangan

hacker, kerentanan keamanan atau hoaks. Layanan ini bertujuan untuk memberikan panduan jangka pendek untuk melindungi sistem atau memulihkan sistem apa pun yang terpengaruh. Sumber informasi pada layanan ini dapat berasal dari sumber pabrikan, berita, milis komunitas dan sumber informasi lainnya.

2) Penanganan insiden siber (*incident handling*)
Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk menerima, menanggapi, dan menganalisis insiden siber.
   a) Koordinasi tanggap insiden siber (*incident response coordination*)
   Adapun layanan penanganan insiden siber dilaksanakan sekurang-kurangnya dengan koordinasi tanggap insiden siber yang terdiri atas kegiatan:
      (1) Menerima informasi terjadinya insiden siber.
      (2) Verifikasi insiden siber.
      (3) Mengklasifikasi insiden siber.
      (4) Koordinasi tanggap insiden siber.
      (5) Menyusun laporan insiden siber.
   Namun apabila Tim Tanggap Insiden Siber memiliki sumber daya lebih, maka Tim Tanggap Insiden Siber dapat memberikan layanan penanganan insiden siber yang lebih dalam seperti dukungan tanggap insiden siber dan analisis insiden siber.
   b) Dukungan tanggap insiden siber (*incident response support*)
   Merupakan sub layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk mengawal dan memberikan pedoman kepada konstituen Tim Tanggap Insiden Siber untuk menangani dan memulihkan insiden siber melalui telepon, *email*, faksimile, atau dokumentasi terkait insiden.
   c) Analisis insiden siber (*incident analysis*)
   Merupakan sub layanan yang diberikan Tim Tanggap Insiden Siber untuk mengamati semua informasi dan artefak digital pada insiden siber yang terjadi. Tujuan analisis ini adalah untuk mengidentifikasi lingkup insiden siber, skala kerusakan yang ditimbulkan insiden siber, kemungkinan terjadinya insiden siber berulang kembali, dan perencanaan tanggap insiden yang mungkin dilakukan untuk menanggulangi insiden siber yang mungkin terjadi. Dalam layanan analisis insiden siber, ada 2 (dua) kegiatan yang mungkin dilakukan sebagai bagian dari sub layanan analisis insiden siber yaitu:
      (1) Pengumpulan bukti forensik (*forensic evidence collection*)
      Merupakan kegiatan yang dilakukan untuk mengoleksi, menyimpan, mendokumentasikan, kemudian menganalisis bukti digital dari sistem yang terkena insiden siber untuk menentukan perubahan terhadap sistem dan

merekonstruksi kejadian yang mungkin menyebabkan sistem terkait mengalami insiden siber.

(2) Pelacakan atau penelusuran (*tracking or tracing*)

Merupakan kegiatan yang menganalisis rekam jejak digital peretas untuk mendapatkan informasi terkait akses yang digunakan oleh peretas, sistem mana yang terserang lebih awal, dan sistem mana lagi yang mungkin terserang dalam lingkup insiden siber terkait.

d) Kunjungan tanggap insiden siber (*incident response on site*)

Merupakan sub layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk mengunjungi secara fisik perangkat yang terinfeksi untuk mendampingi konstituen Tim Tanggap Insiden Siber dalam menangani dan memulihkan insiden siber.

Sedangkan penjelasan untuk layanan tambahan Tim Tanggap Insiden Siber yaitu :

1) Penanganan kerawanan sistem elektronik (*vulnerability handling*)

Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk analisis teknikal yang dilakukan dengan memeriksa kerawanan pada perangkat lunak maupun perangkat keras, serta melakukan proses verifikasi kerawanan yang mungkin dieksploitasi dengan tujuan menyusun rencana untuk memperbaiki kerawanan yang ada. Tim Tanggap Insiden Siber dapat memberikan layanan penanganan kerawanan sistem elektronik yang terdiri atas:

a) Analisis kerawanan sistem elektronik (*vulnerability analysis*)

Merupakan sub layanan Tim Tanggap Insiden Siber dalam bentuk analisis teknikal dan pemeriksaan kerentanan pada perangkat keras atau perangkat lunak. Pemeriksaan kerentanan ini termasuk verifikasi dari kerentanan yang diperkirakan mungkin terjadi dan pemeriksaan teknis baik perangkat keras maupun perangkat lunak untuk menentukan letak spesifik kerentanan dalam sistem yang mungkin dieksploitasi.

b) Tanggap kerawanan sistem elektronik (*vulnerability response*)

Merupakan sub layanan Tim Tanggap Insiden Siber yang dilakukan dengan menentukan respons yang tepat untuk melakukan mitigasi atau perbaikan terhadap suatu kerentanan dalam sistem elektronik. Adapula, pemberian peringatan berupa pengumuman resmi atau distribusi informasi terkait kerentanan merupakan bentuk kegiatan yang dapat dilakukan oleh Tim Tanggap Insiden Siber guna menyebarluaskan strategi untuk melakukan mitigasi terhadap kerentanan sistem elektronik.

c) Koordinasi hasil tanggap kerawanan sistem elektronik (*vulnerability response coordination*)

Merupakan sub layanan Tim Tanggap Insiden Siber yang dilakukan dengan memberikan peringatan dan informasi terkait cara untuk melakukan mitigasi kerentanan dalam sistem kepada pihak lainnya yang terkait dengan sistem agar seluruh pihak mampu berkoordinasi memberikan respon yang tepat dalam menangangi kerentanan sistem elektronik.

2) Penanganan artefak digital (*artifact handling*)

Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk kegiatan analisis teknikal yang dilakukan dengan mencari jejak digital berupa objek atau file yang diduga digunakan untuk melakukan tindakan yang tidak sah terhadap sistem elektronik. Secara umum, artefak digital dapat didefinisikan sebagai objek atau file dalam sistem yang mungkin digunakan penyerang untuk melumpuhkan sistem seperti virus, Trojan Horse, *worms*, *malware*, dan lain-lain. Dalam hal tersedianya sumber daya, Tim Tanggap Insiden Siber dapat memberikan layanan penanganan artefak digital yang terdiri atas :

a) Analisis artefak digital (*artifact analysis*)

Merupakan sub layanan Tim Tanggap Insiden Siber yang dilakukan dengan memeriksa dan menganalisis artefak digital yang mungkin ditemukan dalam sistem. Pemeriksaan yang dilakukan bertujuan untuk mengidentifikasi tipe atau struktur artefak dan membandingkannya dengan artefak yang sudah teridentifikasi oleh Tim Tanggap Insiden Siber pada perbendaharaan artefak untuk dianalisis lebih lanjut agar Tim Tanggap Insiden Siber mampu mengembangkan *patch*.

b) Tanggap artefak digital (*artifact response*)

Merupakan sub layanan Tim Tanggap Insiden Siber yang dilakukan dengan menentukan respons yang tepat dalam mendeteksi dan menghilangkan artefak digital dari dalam sistem untuk pengembangan antivirus atau *Intrusion Detection System* (IDS).

c) Koordinasi hasil tanggap artefak digital (*artifact response coordination*)

Merupakan sub layanan Tim Tanggap Insiden Siber yang dilakukan dengan mendistribusikan informasi dan hasil analisis terkait artefak digital kepada Tim Tanggap Insiden Siber, peneliti, vendor, atau ahli keamanan siber lainnya. Tujuan utama sub layanan ini adalah mengumpulkan dan mendistribusikan temuan-temuan baru terkait artefak digital untuk pengembangan keamanan sistem.

3) Pemberitahuan hasil pengamatan potensi ancaman

Merupakan layanan yang diberikan Tim Tanggap Insiden Siber yang dilakukan dengan menyampaikan ancaman terhadap sistem elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya kepada konstituen.

4) Pendeteksian serangan (*intrusion detection services*)

Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk kegiatan menganalisis data untuk mendeteksi adanya serangan terhadap sistem elektronik atau aktivitas yang mencurigakan terhadap sistem elektronik atau pelanggaran terhadap kebijakan keamanan siber. Sumber data yang menjadi objek analisis dihasilkan dari *Intrusion Detection System* (IDS).

5) Analisis risiko keamanan siber (*risk analysis*)

   Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk kegiatan mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan tindak lanjut untuk menghadapi risiko tersebut.

6) Konsultasi terkait kesiapan penanganan insiden siber

   Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk kegiatan konseling. Layanan ini bertujuan memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan insiden siber.

7) Pembangunan kesadaran dan kepedulian terhadap keamanan siber

   Merupakan layanan yang diberikan Tim Tanggap Insiden Siber dalam bentuk kegiatan diseminasi di bidang keamanan siber kepada konstituen. Tim Tanggap Insiden Siber mungkin dapat mengidentifikasi dimana konstituen memerlukan lebih banyak informasi dan panduan untuk lebih menyesuaikan diri dengan praktik dan kebijakan keamanan di organisasi. Meningkatkan kesadaran keamanan dari konstituen tidak hanya meningkatkan pemahaman tentang masalah keamanan tetapi juga membantu konstituen untuk melakukan kegiatan sehari-hari dengan cara yang lebih aman. Hal ini dapat mengurangi terjadinya serangan dan meningkatkan kemungkinan bahwa konstituen akan mendeteksi dan melaporkan serangan, sehingga mengurangi waktu pemulihan dan menghilangkan atau meminimalkan kerugian. Tim Tanggap Insiden Siber yang melakukan layanan ini mencari peluang untuk meningkatkan kesadaran keamanan melalui:

   a) Pembuatan artikel, poster, buletin, situs web, atau sumber informasi lainnya yang menjelaskan *best practice* keamanan dan memberikan saran tentang tindakan pencegahan yang harus diambil;
   b) Pertemuan berkala dan seminar agar para konstituen tetap mendapat *update* dengan prosedur keamanan yang sedang berlangsung dan potensi ancaman terhadap sistem organisasi; dan
   c) Laporan dan *briefing* untuk pihak manajemen, tidak hanya membahas "keadaan organisasi" dalam hal masalah keamanan komputer tetapi juga untuk mendidik pihak manajemen tentang implikasi dan efek dari mengambil atau tidak mengambil berbagai tindakan keamanan dan tindakan pencegahan. Membangun kesadaran ini juga akan mencakup membantu pihak manajemen untuk memahami masalah keamanan dan strategi mitigasi.

c. Sub Tim Dalam Tim Tanggap Insiden Siber

Di dalam Tim Tanggap Insiden Siber memungkinkan lagi untuk terdapat beberapa sub tim untuk memenuhi layanan-layanan Tim Tanggap Insiden Siber, beberapa jenis sub tim dan kapabilitasnya masing-masing adalah :

1) Sub Tim Penanganan Insiden Siber

   Sub tim ini bertanggung jawab untuk mendeteksi terjadinya insiden siber, menerima informasi terjadinya insiden siber, membuat analisis dasar tingkat ancaman dan dampak yang mungkin ditimbulkan, serta mengumpulkan tim-tim spesialis yang mungkin dibutuhkan dalam menangani masalah yang dihadapi. Sub tim penanganan insiden siber dapat terbagi lagi atas sub tim infrastruktur dan aplikasi.

   a) Sub Tim Infrastruktur

      Sub tim infrastruktur menguasai konsep jaringan dan *host* serta memahami serangan-serangan yang biasanya dilakukan terhadap sebuah infrastruktur sistem elektronik.

   b) Sub Tim Aplikasi

      Sub tim aplikasi memahami seluk-beluk perangkat lunak dan pemrograman yang aman untuk aplikasi.

2) Sub Tim Forensik

   Sub tim forensik mendukung pekerjaan sub tim penanganan insiden siber untuk menentukan bagaimana dan kenapa sebuah insiden siber terjadi serta kerentanan apa yang telah digunakan penyerang serta mengumpulkan bukti-bukti yang diperlukan untuk mengangkat kasus ke ranah hukum apabila diperlukan. Untuk tim berukuran kecil, peran sub tim ini dapat digabungkan dengan sub tim penanganan insiden siber dan peran pengumpulan bukti hukum dapat didelegasikan pada pihak eksternal.

3) Sub Tim Analisis Perangkat Lunak Berbahaya

   Sub tim analisis perangkat lunak berbahaya (*malware*) berfokus pada ancaman berupa program yang bersifat merusak. Sub tim ini bertugas mendata dan membuat profil perangkat lunak berbahaya, menyelidiki cara kerja perangkat lunak berbahaya tertentu, kemudian mengumumkan prosedur penanganannya dan manajemen risiko dari sebuah perangkat lunak berbahaya apabila terjadi insiden siber.

4) Sub Tim Pemburu Ancaman Siber (*Cyber Threat Hunter*)

   Sub tim ini baru dibutuhkan bila Tim Tanggap Insiden Siber mulai bergerak ke arah layanan yang bersifat proaktif. Tugasnya adalah membuat hipotesis dan skenario penyerangan yang mungkin terjadi sehingga organisasi siap menghadapi insiden siber sebelum benar-benar terjadi.

5) Sub Tim Analisis Ancaman

Sub tim ini bertugas melakukan analisis kemungkinan ancaman dari setiap tindakan dan keputusan yang dilakukan organisasi. Misalnya, ketika akan melakukan implementasi kebijakan baru atau migrasi sistem, sub tim ini akan menganalisis celah keamanan apa yang mungkin muncul. Analisis ancaman ini harus dilakukan sesuai keperluan organisasi.

6) Sub Tim Analisis Kerentanan

Sub tim ini berfungsi untuk menyelidiki dan mengkuantifikasi kerentanan sebagai pendukung usaha penanganan insiden siber, kemudian mengimplementasikan pembaharuan perangkat lunak (*patch*) atau metode penguatan (*hardening*) lainnya, menginformasikan perubahan konfigurasi sistem, dan lain sebagainya.

d. Model Tim Tanggap Insiden Siber

Model tim yang mungkin untuk Tim Tanggap Insiden Siber yaitu :

1) Tim Tanggap Insiden Siber Sentral

Tim Tanggap Insiden Siber secara sentral menangani insiden di seluruh organisasi. Model ini efektif untuk organisasi kecil dan untuk organisasi dengan keragaman geografis yang sedikit dalam hal sumber daya komputasi.

2) Tim Tanggap Insiden Siber Terdistribusi

Organisasi memiliki beberapa Tim Tanggap Insiden Siber, masing-masing bertanggung jawab atas segmen logis atau fisik tertentu dari organisasi tersebut. Model ini efektif untuk organisasi besar (misalnya, satu tim per divisi) dan untuk organisasi dengan sumber daya komputasi utama di lokasi yang jauh (misalnya, satu tim per wilayah geografis, satu tim per fasilitas utama). Namun, tim harus menjadi bagian dari entitas yang terkoordinasi sehingga proses penanganan insiden siber konsisten di seluruh organisasi dan informasi dapat dibagikan antara tim. Hal tersebut sangat penting karena banyak tim yang dapat melihat komponen dari insiden yang sama atau mungkin menangani insiden siber serupa.

3) Tim Tanggap Insiden Siber Koordinasi

Tim Tanggap Insiden Siber model ini tidak memiliki sumber daya untuk menangani insiden siber, sehingga Tim Tanggap Insiden Siber akan berkoordinasi dengan Tim Tanggap Insiden Siber lainnya untuk meminta bantuan. Model ini merupakan model Tim Tanggap Insiden Siber yang paling minimalis yang bisa dibentuk.

e. Sumber Daya Tim Tanggap Insiden Siber

1) Sumber Daya Tim Tanggap Insiden Siber

Sumber daya yang diperlukan Tim Tanggap Insiden Siber untuk menyelenggarakan layanan, yaitu:

a) sumber daya manusia.
b) perangkat pendukung.

c) pendanaan.

2) Sumber Daya Manusia Tim Tanggap Insiden Siber

Untuk membangun Tim Tanggap Insiden Siber dengan kemampuan penanganan insiden yang cakap, dibutuhkan SDM Tim Tanggap Insiden Siber dengan serangkaian keterampilan dan keahlian teknis tertentu yang memungkinkan untuk merespon insiden, melakukan analisis, dan berkomunikasi secara efektif dengan konstituen dan kontak eksternal lainnya. SDM Tim Tanggap Insiden Siber juga harus kompeten dalam memecahkan masalah, harus mudah beradaptasi dengan perubahan, dan harus efektif dalam kegiatan Tim Tanggap Insiden Siber sehari-hari. Keterampilan yang perlu dimiliki SDM Tim Tanggap Insiden Siber, dibagi menjadi 2 (dua) kelompok besar : keterampilan pribadi (*personal skills*) dan keterampilan teknis (*technical skills*). SDM Tim Tanggap Insiden Siber diharapkan memiliki kompetensi minimum untuk melakukan pekerjaan dan efektif dalam tanggung jawab pekerjaannya.

a) Keterampilan pribadi (*personal skills*)

Penting bagi anggota Tim Tanggap Insiden Siber untuk memiliki berbagai keterampilan pribadi karena bagian utama dari kegiatan penanganan akan melibatkan komunikasi dengan konstituen, anggota Tim Tanggap Insiden Siber sendiri, tim Tim Tanggap Insiden Siber lain, berbagai pakar teknis, dan individu lain yang mungkin memiliki berbagai tingkat pemahaman teknis yang berbeda. Keterampilan pribadi akan berkontribusi terhadap reputasi dan keberhasilan anggota Tim Tanggap Insiden Siber secara keseluruhan maupun dalam interaksi sehari-harinya. Misalnya, anggota Tim Tanggap Insiden Siber yang kompeten secara teknis dan memiliki keterampilan komunikasi yang baik dapat memperkuat reputasi dan rasa hormat terhadap Tim Tanggap Insiden Siber (baik oleh konstituen maupun oleh orang lain yang berinteraksi dengan Tim Tanggap Insiden Siber). SDM Tim Tanggap Insiden Siber tersebut juga bisa menjadi panutan bagi SDM Tim Tanggap Insiden Siber lainnya. Di sisi lain, apabila anggota Tim Tanggap Insiden Siber memiliki keterampilan komunikasi yang buruk dapat mengakibatkan miskomunikasi yang dapat merusak reputasi dan posisi Tim Tanggap Insiden Siber di masyarakat, terutama ketika komunikasi tersebut disalahartikan atau salah penanganan. Berikut ini adalah keterampilan pribadi yang dibutuhkan anggota Tim Tanggap Insiden Siber, yaitu:

(1) Komunikasi (*communication*)

Kemampuan untuk berkomunikasi secara efektif adalah komponen penting dari keterampilan pribadi yang dibutuhkan oleh anggota Tim Tanggap Insiden Siber. Anggota Tim Tanggap Insiden Siber perlu menjadi komunikator yang efektif untuk memastikan bahwa anggota Tim Tanggap Insiden Siber memperoleh dan memberikan informasi yang diperlukan. Anggota Tim Tanggap Insiden Siber juga

harus menjadi pendengar yang baik, memahami apa yang dikatakan (atau tidak dikatakan) untuk memungkinkan mereka memperoleh detail tentang insiden yang dilaporkan. Anggota Tim Tanggap Insiden Siber juga harus tetap mengendalikan komunikasi ini untuk paling efektif menentukan apa yang terjadi, fakta apa yang penting, dan bantuan apa yang diperlukan. Anggota Tim Tanggap Insiden Siber harus mampu beradaptasi dengan tingkat diskusi yang sesuai tanpa direndahkan atau berbicara di atas tingkat pemahaman pendengar (apakah pendengarnya adalah pengguna *end user*, administrator, manajer, atau anggota komunitas).

(a) Komunikasi tertulis

Bagi banyak Tim Tanggap Insiden Siber, sebagian besar komunikasinya terjadi melalui kata-kata tertulis. Komunikasi ini dapat berupa berbagai bentuk, termasuk:

- Tanggapan dalam *email* tentang insiden.
- Dokumentasi laporan peristiwa atau insiden, kerentanan, dan informasi teknis lainnya.
- Pemberitahuan dan/atau pedoman yang diberikan kepada konstituen.
- Pengembangan internal terhadap kebijakan dan prosedur Tim Tanggap Insiden Siber.
- Komunikasi eksternal lainnya kepada anggota, manajemen, atau pihak terkait lainnya.

Anggota Tim Tanggap Insiden Siber harus dapat menulis dengan jelas dan singkat, menggambarkan kegiatan secara akurat, dan memberikan informasi yang mudah dipahami pembaca.

(b) Komunikasi Lisan

Kemampuan untuk berkomunikasi secara efektif melalui komunikasi lisan juga merupakan keterampilan yang penting untuk memastikan bahwa anggota Tim Tanggap Insiden Siber dapat mengatakan kata-kata yang tepat kepada orang yang tepat. Komunikasi lisan sering terjadi melalui pertukaran telepon atau diskusi tatap muka dan dapat melibatkan berbagai individu, misalnya:

- Anggota Tim Tanggap Insiden Siber lainnya.
- Administrator sistem dan jaringan (atau anggota TI lainnya).
- Pemilik/pengembang aplikasi.
- Konstituen.
- Subjek atau pakar teknis.
- Petugas keamanan.
- Manajemen atau anggota administrasi lainnya.

- Anggota sumber daya manusia.
- Anggota hukum atau penegak hukum.
- Anggota pers/media/humas.
- Vendor.

Dalam beberapa kasus, anggota Tim Tanggap Insiden Siber yang dipilih mungkin menjadi kontak utama dengan kelompok-kelompok di atas dan/atau melayani peran "juru bicara resmi" untuk Tim Tanggap Insiden Siber, mempresentasikan misi dan tujuan Tim Tanggap Insiden Siber, dan berbicara secara otoritatif tentang layanan dan kegiatan yang dilakukan oleh Tim Tanggap Insiden Siber.

Baik komunikasi melalui telepon, secara langsung, atau melalui media cetak, maka metode komunikasi, bahasa, dan nada suara yang digunakan anggota Tim Tanggap Insiden Siber harus tetap profesional, tenang, dan percaya diri.

(2) Keterampilan presentasi (*presentation skills*)

Meskipun semua anggota yang menangani insiden Tim Tanggap Insiden Siber dapat berinteraksi setiap hari dengan konstituen, mungkin tidak semua anggota Tim Tanggap Insiden Siber merasa nyaman ketika harus melakukan presentasi di depan audiens dalam jumlah besar atau audiens dari Tim Tanggap Insiden Siber sendiri. Selain itu, anggota Tim Tanggap Insiden Siber mungkin menghadapi situasi sulit, kontroversial, atau berpotensi bermusuhan yang harus ditangani secara profesional. Oleh karena itu, anggota Tim Tanggap Insiden Siber harus dalam merespon secara efektif tanpa merusak reputasi Tim Tanggap Insiden Siber atau menyinggung orang lain. Agar anggota Tim Tanggap Insiden Siber menjadi kepercayaan diri untuk melakukan presentasi tentu membutuhkan waktu dan upaya, dengan demikian anggota Tim Tanggap Insiden Siber diharapkan lebih berpengalaman dan nyaman dalam situasi seperti ini.

Tim Tanggap Insiden Siber sering membutuhkan 1 (satu) atau beberapa anggota dengan keterampilan presentasi yang baik. Keterampilan ini mungkin diperlukan untuk melakukan presentasi teknis, penjelasan ke pihak manajemen atau sponsor, diskusi panel di konferensi/seminar, atau bentuk lain dari keterlibatan berbicara di depan umum. Keterampilan ini dapat diperluas, misalnya, untuk memberikan kesaksian ahli dalam proses hukum atau lainnya atas nama Tim Tanggap Insiden Siber atau anggota konstituen. Anggota Tim Tanggap Insiden Siber ini dapat mewakili Tim Tanggap Insiden Siber dan seringkali perlu menjelaskan misi dan tujuan, layanan, arahan strategis, dan lainnya. Anggota

Tim Tanggap Insiden Siber yang berpengetahuan tersebut juga memahami bahwa setiap konflik yang ditemui mungkin merupakan hasil dari frustrasi dengan masalah spesifik yang sedang diperdebatkan, kebijakan dan prosedur tim, organisasi, atau bahkan pihak lain yang mungkin terkait dengan Tim Tanggap Insiden Siber dengan cara tertentu. Anggota Tim Tanggap Insiden Siber yang berpengetahuan tersebut memahami kebutuhan untuk tetap tenang, menjaga isu-isu dalam perspektif, mewakili Tim Tanggap Insiden Siber dan/atau konstituen yang dilayani dengan tepat, dan tidak mengambil pertanyaan dan interaksi yang mengakibatkan bermusuhan yang bersifat personal.

(3) Diplomasi (*diplomacy*)

Anggota Tim Tanggap Insiden Siber sering menemukan bahwa pihak lain yang sering berinteraksi dengan Tim Tanggap Insiden Siber mungkin memiliki berbagai tujuan dan kebutuhan. Pihak lain ini mungkin memiliki berbagai tingkat pengetahuan, tingkat emosional, dan integritas yang berbeda-beda. Anggota Tim Tanggap Insiden Siber yang terampil akan dapat mengantisipasi titik-titik pertengkaran yang potensial, dapat merespons dengan tepat, menjaga hubungan baik, dan menghindari menyinggung orang lain. Anggota Tim Tanggap Insiden Siber juga akan diharapkan memahami bahwa pihak lain tersebut mewakili Tim Tanggap Insiden Siber dan/atau organisasi. Maka, dalam hal ini diperlukan diplomasi sekaligus kebijaksanaan.

(4) Kemampuan untuk mengikuti kebijakan dan prosedur (*ability to follow policies and procedures*)

Keterampilan penting lainnya yang dibutuhkan oleh anggota Tim Tanggap Insiden Siber adalah kemampuan untuk mengikuti dan mendukung kebijakan dan prosedur yang ditetapkan organisasi atau tim. Dari perspektif historis, anggota Tim Tanggap Insiden Siber harus memahami bagaimana dan mengapa kebijakan dan prosedur muncul. Untuk memastikan layanan respons insiden yang konsisten dan dapat diandalkan, anggota Tim Tanggap Insiden Siber harus siap untuk menerima dan mengikuti aturan dan pedoman, bahkan jika ini tidak sepenuhnya didokumentasikan. Di sisi lain, jika dirasa perlu melakukan perubahan, maka diperlukan prosedur manajemen perubahan agar perubahan akan meningkatkan kualitas operasi Tim Tanggap Insiden Siber dan memberikan manfaat pada konstituensi yang dilayani.

(5) Keterampilan tim (*team skills*)

Anggota Tim Tanggap Insiden Siber harus dapat bekerja di lingkungan tim secara produktif dan bersikap kooperatif. Anggota Tim Tanggap Insiden Siber perlu menyadari tanggung jawab yang dimilikinya, berkontribusi pada tujuan tim dan bekerja bersama untuk berbagi informasi, beban kerja, dan pengalaman. Anggota Tim Tanggap Insiden Siber juga harus fleksibel dan mau beradaptasi dengan perubahan. Anggota Tim Tanggap Insiden Siber membutuhkan keterampilan tim untuk berinteraksi dengan pihak lain (misalnya, anggota Tim Tanggap Insiden Siber lainnya dan anggota organisasi lainnya, seperti unit kerja TI, petugas keamanan pada situs dan operator jaringan). Jika seorang anggota Tim Tanggap Insiden Siber tidak mau bekerja sama dan mendukung anggota Tim Tanggap Insiden Siber lainnya, maka moral Tim Tanggap Insiden Siber akan terpengaruh, dan mungkin ada kebencian di antara anggota Tim Tanggap Insiden Siber yang lain. Kekesalan ini dapat mengakibatkan hilangnya produktivitas tim, efektivitas, reputasi, atau potensi hilangnya anggota Tim Tanggap Insiden Siber lainnya (yang mengundurkan diri dari jabatan karena tidak puas dengan lingkungan kerja).

Ketika Tim Tanggap Insiden Siber berkembang dan tumbuh, mungkin ada kebutuhan untuk 1 (satu) atau lebih anggota Tim Tanggap Insiden Siber yang dapat bertindak dalam peran kepemimpinan untuk mendukung tim teknis dalam Tim Tanggap Insiden Siber. Para pemimpin ini mengelola kegiatan sehari-hari anggota di tim yang lebih kecil dan juga bekerja dengan manajer Tim Tanggap Insiden Siber mengenai keputusan yang berkaitan dengan arahan strategis, kebijakan Tim Tanggap Insiden Siber, infrastruktur, dan/atau tindakan operasional yang membutuhkan lebih dari latar belakang teknis untuk mengidentifikasi pendekatan terbaik.

Anggota Tim Tanggap Insiden Siber yang memiliki kemampuan teknis dan keterampilan manajemen/kepemimpinan tidak mudah ditemukan. Anggota Tim Tanggap Insiden Siber dapat memperoleh kepemimpinan dari waktu ke waktu melalui pengalaman dan pelatihan. Dan penting untuk menyadari bahwa kepemimpinan bukanlah keterampilan yang tiba-tiba tersedia sesuai permintaan setelah seseorang mengikuti kelas pelatihan kepemimpinan. Sebaliknya, kepemimpinan adalah sesuatu yang perlu waktu untuk dipelihara dan dikembangkan atau dicari (di luar Tim Tanggap Insiden Siber). Pihak manajemen mungkin perlu memberikan dukungan untuk posisi kepemimpinan di Tim Tanggap Insiden Siber.

(6) Integritas (*integrity*)

Dalam pekerjaan Tim Tanggap Insiden Siber, anggota Tim Tanggap Insiden Siber sering berurusan dengan informasi yang bersifat sensitif dan mungkin memiliki akses ke informasi yang layak diberitakan. Anggota Tim Tanggap Insiden Siber harus dapat dipercaya dan mampu menangani informasi secara rahasia sesuai dengan pedoman Tim Tanggap Insiden Siber, setiap perjanjian atau peraturan konstituen, dan/atau kebijakan dan prosedur organisasi apa pun.

Dalam upaya memberikan penjelasan atau tanggapan teknis, anggota Tim Tanggap Insiden Siber harus berhati-hati untuk memberikan informasi yang tepat dan akurat untuk menghindari penyebaran informasi rahasia/terbatas apa pun yang dapat merusak reputasi organisasi, sehingga berakibat pada hilangnya integritas Tim Tanggap Insiden Siber atau berpengaruh pada kegiatan yang melibatkan pihak lain.

Dengan demikian, adalah penting bahwa anggota Tim Tanggap Insiden Siber memahami perbedaan antara peran terkait layanan Tim Tanggap Insiden Siber yaitu memberikan bantuan kepada konstituen Tim Tanggap Insiden Siber dan kebutuhan untuk memastikan bahwa informasi dilindungi dan ditangani dengan tepat. Meskipun anggota Tim Tanggap Insiden Siber mengetahui tentang informasi dan dapat mengomentari suatu topik, tetapi apabila mengungkapkan informasi yang bersifat rahasia/terbatas maka akan dapat memengaruhi penyelidikan yang sedang berlangsung. Anggota Tim Tanggap Insiden Siber harus tetap sadar akan tanggung jawabnya dan tidak bersikap lengah dan tidak melakukan pengungkapan yang tidak sah.

(7) Mengetahui batasan seseorang (*knowing one's limits*)

Kemampuan penting lain yang harus dimiliki anggota Tim Tanggap Insiden Siber adalah untuk dapat dengan mudah mengakui ketika telah mencapai batas pengetahuan atau keahlian yang dimiliki. Betapapun sulitnya mengakui keterbatasan, anggota Tim Tanggap Insiden Siber harus mengenali keterbatasan yang dimiliki dan secara aktif mencari dukungan dari anggota Tim Tanggap Insiden Siber lainnya, pakar lain, atau pihak manajemen. Jika tidak, reputasi Tim Tanggap Insiden Siber dapat sangat dipengaruhi oleh anggota Tim Tanggap Insiden Siber yang telah memberikan informasi atau panduan yang salah kepada orang lain.

(8) Mengatasi stres (*coping with stress*)

Anggota Tim Tanggap Insiden Siber sering berada dalam situasi yang penuh tekanan. Anggota Tim Tanggap Insiden Siber harus dapat mengenali diri sendiri

ketika menjadi stres, bersedia membuat sesama anggota Tim Tanggap Insiden Siber menyadari situasi dan mengambil langkah-langkah yang diperlukan (atau mencari bantuan) untuk mengendalikan dan menjaga ketenangan diri. Secara khusus, anggota Tim Tanggap Insiden Siber membutuhkan kemampuan untuk tetap tenang dalam situasi tegang sekalipun, mulai dari beban kerja yang berlebihan, menghadapi konstituen yang agresif, hingga menghadapi insiden yang mungkin berisiko terhadap kehidupan manusia atau infrastruktur kritis. Reputasi Tim Tanggap Insiden Siber dan reputasi anggota Tim Tanggap Insiden Siber sebagai individu akan meningkat atau justru menderita tergantung pada bagaimana situasi tersebut ditangani.

(9) Penyelesaian masalah (*problem solving*)

Anggota Tim Tanggap Insiden Siber terkadang dihadapkan dengan data dan volume informasi yang besar di setiap harinya. Penting bagi anggota Tim Tanggap Insiden Siber untuk dapat melakukan hal berikut:

- Menentukan relevansi data yang tersedia.
- Mengidentifikasi informasi apa yang penting, hilang, atau mungkin menyesatkan atau salah.
- Memutuskan bagaimana cara menangani data itu.

Tanpa keterampilan pemecahan masalah yang baik, anggota Tim Tanggap Insiden Siber dapat menjadi kewalahan dengan volume data yang terkait dengan insiden dan tugas-tugas lain yang perlu ditangani. Keterampilan pemecahan masalah juga mencakup kemampuan bagi anggota Tim Tanggap Insiden Siber untuk berpikir *out of the box* atau melihat masalah dari berbagai perspektif untuk mengidentifikasi informasi atau data yang relevan. Keterampilan ini termasuk, misalnya:

- Mengetahui siapa saja dalam Tim Tanggap Insiden Siber yang dapat dihubungi atau dekati untuk informasi tambahan, ide kreatif, atau menambah wawasan teknis.
- Mengenali dan mencari informasi tambahan dari sumber lainnya (misalnya, studi literatur, informasi insiden di masa lalu yang mungkin serupa, kesamaan dalam teknik atau *tools* serangan, dan lainnya).
- Memverifikasi informasi melalui pendekatan alternatif.
- Menyederhanakan informasi untuk menentukan hubungan atau untuk mengkorelasikan informasi dengan data insiden lainnya.

(10) Manajemen waktu (*time management*)

Seiring dengan keterampilan memecahkan masalah, penting bagi anggota Tim Tanggap Insiden Siber untuk dapat mengatur waktu secara efektif. Anggota Tim Tanggap Insiden Siber akan dihadapkan dengan banyak tugas mulai dari menganalisis, mengoordinasikan, dan menanggapi insiden, hingga melakukan tugas-tugas seperti memprioritaskan beban kerja, menghadiri dan/atau mempersiapkan rapat, melengkapi absensi, mengumpulkan statistik, melakukan penelitian, memberikan pengarahan dan presentasi, bepergian ke konferensi, dan mungkin memberikan dukungan teknis di lokasi terjadinya insiden secara *on-site*.

Agar tetap produktif, maka anggota Tim Tanggap Insiden Siber harus dapat menyeimbangkan upaya antara menyelesaikan tugas yang diberikan, mengakui kapan harus mencari bantuan atau bimbingan dari pihak manajemen (ketika beban kerja menjadi luar biasa), dan menghindari keadaan di mana secara anggota Tim Tanggap Insiden Siber memprioritaskan tugas baru yang muncul karena ini akan mencegah anggota Tim Tanggap Insiden Siber dari benar-benar menyelesaikan tugas yang diberikan.

b) Keterampilan teknis (*technical skills*)

Keterampilan teknis yang dibutuhkan anggota Tim Tanggap Insiden Siber telah dipisahkan menjadi 2 (dua) kategori: keterampilan teknis dasar (*technical foundation skills*) dan keterampilan penanganan insiden (*incident handling skills*). Kompetensi teknis dasar membutuhkan pemahaman dasar tentang teknologi yang digunakan oleh Tim Tanggap Insiden Siber dan konstituen, serta pemahaman tentang masalah yang memengaruhi Tim Tanggap Insiden Siber atau konstituen. Masalah-masalah tersebut antara lain:

- Jenis insiden yang dilaporkan atau dilihat oleh masyarakat.
- Bagaimana penyediaan layanan Tim Tanggap Insiden Siber (tingkat dan kedalaman bantuan teknis disediakan untuk konstituen).
- Respons yang sesuai untuk Tim Tanggap Insiden Siber (misalnya, prosedur atau regulasi apa yang harus dipertimbangkan atau dipatuhi saat melakukan tanggap insiden).
- Tingkat wewenang yang dimiliki Tim Tanggap Insiden Siber dalam mengambil tindakan spesifik apa pun ketika menerapkan solusi teknis untuk insiden yang dilaporkan ke Tim Tanggap Insiden Siber.

Sedangkan keterampilan penanganan insiden memerlukan pemahaman tentang teknik, poin keputusan, dan alat pendukung (perangkat lunak atau aplikasi) yang diperlukan dalam pekerjaan harian Tim Tanggap Insiden Siber.

(1) Keterampilan teknis dasar (*technical foundation skills*)

(a) Prinsip keamanan (*security principles*)

Anggota anggota Tim Tanggap Insiden Siber perlu memiliki pemahaman umum tentang prinsip-prinsip keamanan dasar seperti :

- Kerahasiaan (*confidentiality*).
- Ketersediaan (*availability*).
- Otentikasi (*authentication*).
- Integritas (*integrity*).
- Kontrol akses (*access control*).
- Privasi (*privacy*).
- Non-repudiation (*non-repudiation*).

Pengetahuan tentang prinsip-prinsip keamanan diperlukan bagi anggota Tim Tanggap Insiden Siber untuk memahami masalah potensial yang dapat muncul jika langkah-langkah keamanan yang tepat belum diterapkan dengan benar, serta dampak potensial terhadap sistem konstituen atau sistem Tim Tanggap Insiden Siber. Anggota Tim Tanggap Insiden Siber dengan pemahaman ini akan lebih siap untuk menentukan kebutuhan konstituennya dalam sistem konfigurasi yang aman untuk mencegah penyalahgunaan atau kompromi dan juga lebih siap untuk memberikan bantuan teknis dan bimbingan yang tepat ketika pelanggaran terjadi.

(b) Kerentanan/kelemahan keamanan (*security vulnerabilities/weaknesses*)

Untuk memahami bagaimana setiap serangan spesifik dimanifestasikan dalam teknologi perangkat lunak atau perangkat keras, maka anggota Tim Tanggap Insiden Siber harus dapat terlebih dahulu memahami penyebab mendasar dari kerentanan yang dieksploitasi sehingga menyebabkan serangan siber. Kemampuan untuk mengenali dan mengkategorikan jenis kerentanan yang paling umum dan serangan terkait yang mungkin melibatkan:

- Masalah keamanan fisik.
- Kekurangan desain protokol (misalnya, *man-in-the-middle attack*, *spoofing*).
- Kode berbahaya (misalnya, virus, *worm*, *trojan horse*).
- Cacat implementasi (misalnya, *buffer overflow* dan *timing windows*).
- Kelemahan konfigurasi.
- Kesalahan atau ketidakpedulian pengguna.

(c) Internet

Anggota Tim Tanggap Insiden Siber juga penting untuk memahami internet. Tanpa informasi latar belakang mendasar ini, maka pemahaman tentang memahami masalah teknis lainnya, seperti kurangnya keamanan dalam protokol dan layanan mendasar yang digunakan di internet atau untuk mengantisipasi ancaman yang mungkin terjadi di masa depan. Paling tidak, anggota Tim Tanggap Insiden Siber harus tahu tentang sejarah, filosofi, dan struktur internet, dan infrastruktur yang mendukungnya.

(d) Risiko (*risks*)

Anggota Tim Tanggap Insiden Siber perlu memiliki pemahaman dasar tentang analisis risiko keamanan siber, seperti mengenali berbagai jenis risiko, serta menilai tingkat dampak dan kemungkinan atas terjadinya risiko. Anggota Tim Tanggap Insiden Siber yang baru direkrut mungkin tidak memiliki pengetahuan ini dan membutuhkan bimbingan dan pendampingan untuk memahami risiko yang mungkin memengaruhi konstituen yang dilayani, serta risiko apa pun yang mungkin memengaruhi Tim Tanggap Insiden Siber itu sendiri.

(e) Protokol jaringan (*network protocol*)

Anggota Tim Tanggap Insiden Siber perlu memiliki pemahaman dasar tentang protokol jaringan yang digunakan oleh Tim Tanggap Insiden Siber dan konstituen. Pada setiap protokol harus dimiliki pemahaman dasar tentang protokol, spesifikasinya, dan bagaimana protokol itu digunakan. Selain itu, anggota Tim Tanggap Insiden Siber harus memahami jenis ancaman atau serangan terhadap protokol, serta strategi untuk mengurangi atau menghilangkan serangan tersebut.

Minimal anggota Tim Tanggap Insiden Siber harus terbiasa dengan protokol seperti IP, TCP, UDP, ICMP, ARP, dan RARP. Anggota Tim Tanggap Insiden Siber harus memahami bagaimana protokol ini bekerja, untuk apa protokol digunakan, perbedaan di antaranya, beberapa kelemahan umum, dan lain-lain. Selain itu, anggota Tim Tanggap Insiden Siber harus memiliki pemahaman yang sama tentang protokol seperti TFTP, FTP, HTTP, HTTPS, SNMP, SMTP, dan protokol lain apa pun yang digunakan oleh Tim Tanggap Insiden Siber atau konstituennya.

Keterampilan spesialis mencakup pemahaman yang lebih mendalam tentang konsep dan prinsip keamanan di semua bidang di atas selain pengetahuan ahli dalam mekanisme dan teknologi yang mengarah pada

kelemahan dalam protokol ini, kelemahan yang dapat dieksploitasi (dan mengapa), jenis metode eksploitasi yang kemungkinan akan digunakan, dan strategi untuk mengurangi atau menghilangkan potensi masalah ini. Anggota Tim Tanggap Insiden Siber akan memiliki pemahaman ahli tentang protokol tambahan atau teknologi internet (DNSSEC, IPv6, IPSEC, standar telekomunikasi lainnya yang mungkin diterapkan atau berinteraksi dengan jaringan konstituen mereka, seperti ATM, BGP, *broadband*, *Voice over* IP, teknologi nirkabel, protokol *routing* lainnya, atau teknologi baru yang muncul, dan lainnya) dan memberikan bimbingan teknis ahli kepada anggota Tim Tanggap Insiden Siber atau konstituen lainnya.

(f) Aplikasi dan layanan jaringan (*networks application and services*)

Anggota Tim Tanggap Insiden Siber memerlukan pemahaman dasar tentang aplikasi dan layanan jaringan yang umum digunakan oleh Tim Tanggap Insiden Siber dan konstituen (DNS, NFS, SSH, dan lainnya). Untuk setiap aplikasi atau layanan, Anggota Tim Tanggap Insiden Siber harus memahami tujuan aplikasi atau layanan tersebut, cara kerjanya, penggunaan umum, konfigurasi aman, dan jenis ancaman atau serangan terhadap aplikasi atau layanan, serta strategi mitigasi.

Keterampilan ini meliputi wawasan teknis pada aplikasi dan layanan, serta produk baru yang dapat diintegrasikan ke dalam konstituensi Tim Tanggap Insiden Siber. Keterampilan ini juga meliputi pemberian wawasan tentang masalah dan pertimbangan keamanan yang perlu didiskusikan, diatasi, atau diselesaikan dalam mengimplementasikan sistem apa pun yang ada atau baru, aplikasi baru, atau desain arsitektur jaringan. Di tingkat spesialis, pemahaman juga mencakup: pengalaman dari hal lainnya, aplikasi yang jarang digunakan, layanan yang sudah usang namun masih digunakan, dan layanan yang dianggap menarik bagi Tim Tanggap Insiden Siber atau konstituen.

(g) Permasalahan keamanan jaringan (*network security issues*)

Anggota Tim Tanggap Insiden Siber harus memiliki pemahaman dasar tentang konsep keamanan jaringan dan dapat mengenali titik-titik rawan dalam konfigurasi jaringan. Anggota Tim Tanggap Insiden Siber harus memahami konsep dan keamanan perimeter dasar *firewall* jaringan (desain, *packet filtering*, sistem *proxy*, DMZ, *bastion host*, dan lainnya), keamanan *router*, potensi untuk pengungkapan informasi data yang melewati seluruh

jaringan (misalnya, pemantauan paket atau *sniffers*), atau ancaman yang berkaitan dengan menerima informasi yang tidak dapat dipercaya.

Keterampilan ini meliputi kemampuan untuk mengantisipasi, mengidentifikasi, mengisolasi, dan menggambarkan potensi kerentanan baru yang dapat mempengaruhi konstituen (atau Tim Tanggap Insiden Siber itu sendiri) sebagai akibat dari perubahan dalam desain jaringan, perangkat keras, atau perangkat lunak. Anggota Tim Tanggap Insiden Siber diharapkan dapat mengidentifikasi dan mengembangkan *tools* atau proses yang akan mengurangi atau menyelesaikan kelemahan keamanan potensial ini.

(h) Masalah keamanan *host*/sistem (*host/system security issues*)

Selain memahami masalah keamanan di tingkat jaringan, anggota Tim Tanggap Insiden Siber perlu memahami masalah keamanan di tingkat *host* untuk berbagai jenis sistem operasi (UNIX, Windows, atau sistem operasi lainnya yang digunakan oleh Tim Tanggap Insiden Siber atau konstituen). Sebelum memahami aspek keamanan, anggota Tim Tanggap Insiden Siber harus terlebih dahulu memiliki :

- Pengalaman menggunakan sistem operasi (masalah keamanan pengguna).
- Pengalaman dengan mengelola dan memelihara sistem operasi (sebagai administrator).

Kemudian, untuk setiap sistem operasi, anggota Tim Tanggap Insiden Siber perlu memahami cara untuk:

- Mengkonfigurasi sistem dengan aman (*hardening*).
- Meninjau file konfigurasi untuk mengetahui kelemahan keamanan.
- Mengidentifikasi metode serangan umum.
- Menentukan apakah terdapat upaya untuk mengkompromikan sistem.
- Menentukan apakah upaya untuk mengkompromikan sistem berhasil atau tidak.
- Meninjau file *log* untuk mengetahui anomali.
- Menganalisis hasil serangan.
- Mengelola hak istimewa pada sistem.
- Mengamankan daemon jaringan.
- Terpulihkan dari keadaan terkompromi.

(i) Kode berbahaya (program virus, *worm, trojan horse*)

Anggota Tim Tanggap Insiden Siber harus memahami berbagai jenis serangan kode berbahaya yang terjadi dan bagaimana hal ini dapat memengaruhi konstituen (sistem yang terkompromi, *denial of service*, hilangnya integritas data, dan lainnya). Kode berbahaya dapat memiliki berbagai jenis muatan *denial of service* yang dapat menyebabkan serangan atau *web defacement*, atau kode tersebut dapat memuat lebih banyak muatan dinamis yang dapat dikonfigurasi untuk menghasilkan vektor serangan berbagai sisi. Anggota Tim Tanggap Insiden Siber harus memahami tidak hanya bagaimana kode berbahaya disebarkan melalui beberapa metode yang jelas (*disk*, *email*, program, dan lainnya), tetapi juga bagaimana kode berbahaya dapat menyebar melalui cara lain seperti PostScript, macro pada Microsoft Office, MIME, *file* berbagi *peer-to-peer*, atau virus pada sektor *boot*. Anggota Tim Tanggap Insiden Siber harus mengetahui bagaimana serangan tersebut terjadi dan diperbanyak, risiko dan kerusakan yang terkait dengan serangan tersebut, strategi pencegahan dan mitigasi, proses deteksi dan pemindahan, dan teknik pemulihan.

Keterampilan ini mencakup kemampuan dalam melakukan analisis, pengujian *black box*, atau *reverse engineering* pada kode berbahaya yang terkait dengan serangan tersebut dan dalam memberikan saran kepada Tim Tanggap Insiden Siber tentang pendekatan terbaik untuk tanggap insiden yang efektif.

(j) Keterampilan pemrograman (*programming skills*)

Beberapa anggota Tim Tanggap Insiden Siber perlu memiliki pengalaman pemrograman sistem dan jaringan. Tim harus memastikan bahwa serangkaian bahasa pemrograman dicakup pada sistem operasi yang digunakan tim dan konstituen. Misalnya, Tim Tanggap Insiden Siber harus memiliki pengalaman terkait bahasa pemrograman berikut:

- C.
- Perl.
- Awk.
- Java.
- Shell (berbagai variasi).
- *Tools script* lainnya.

Script atau perangkat bahasa pemrograman ini dapat digunakan untuk membantu dalam analisis dan penanganan informasi insiden (misalnya,

menulis *script* yang berbeda untuk menghitung dan memilah berbagai *log*, mencari basis data, mencari informasi, mengekstraksi informasi dari *log/file*, mengumpulkan dan menggabungkan data).

Selain itu, anggota Tim Tanggap Insiden Siber harus memahami konsep dan teknik pemrograman yang aman. Anggota Tim Tanggap Insiden Siber perlu menyadari bagaimana kerentanan dapat dimasukkan ke dalam kode (misalnya, melalui praktik pemrograman dan desain yang buruk) dan bagaimana menghindarinya dalam *tools* atau produk apa pun yang mungkin dikembangkan untuk Tim Tanggap Insiden Siber atau konstituen.

Keterampilan spesialis meliputi keterampilan dalam pengembangan perangkat lunak dan pemrograman dalam berbagai bahasa pemrograman.

(2) Keterampilan penanganan insiden (*incident handling skills*)

1) Kebijakan dan prosedur tim tanggap insiden siber lokal (*local team policies and procedures*)

Anggota Tim Tanggap Insiden Siber harus dilatih dalam kebijakan dan prosedur lokal yang mengatur bagaimana operasional Tim Tanggap Insiden Siber dijalankan. Setiap pekerjaan diharapkan mengikuti kebijakan atau prosedur atau sesuai arahan lain dari pihak manajemen. Anggota Tim Tanggap Insiden Siber membutuhkan informasi dasar mengani ini dan harus memiliki perpegang teguh terhadap tentang prinsip-prinsip panduan, jika tidak, maka anggota Tim Tanggap Insiden Siber tidak akan memahami kerangka kerja dan batasan-batasan bagi Tim Tanggap Insiden Siber. Anggota Tim Tanggap Insiden Siber harus dapat mendukung kebijakan dan prosedur ini, tidak hanya di tingkat Tim Tanggap Insiden Siber tetapi juga di tingkat organisasi.

2) Memahami/mengidentifikasi teknik penyusup (*understanding/ identifying intruder techniques*)

Membangun keterampilan teknis dasar, anggota Tim Tanggap Insiden Siber harus dapat mengenali teknik intrusi yang diketahui berdasarkan jejak digital atau artefak yang ditinggalkan oleh berbagai jenis serangan dalam laporan insiden yang ditangani. Selain itu, anggota Tim Tanggap Insiden Siber perlu mengetahui metode yang tepat untuk melindungi terhadap teknik serangan yang diketahui dan risiko yang terkait dengan serangan tersebut.

Mengingat data insiden adalah nyata, maka anggota Tim Tanggap Insiden Siber harus dapat menggunakan pengetahuan yang telah dikumpulkan dari

analisis yang ada yang terdokumentasi untuk mengidentifikasi jenis serangan dan mengenali alat pengganggu khusus atau *toolkit*, teknik yang digunakan, atau kode berbahaya lainnya. Dengan setiap jenis serangan, Anggota Tim Tanggap Insiden Siber harus memahami risiko dan efek yang terkait, tingkat keparahan relatif, dan metode mitigasi, pencegahan, atau pemulihan.

Keahlian penanganan insiden penting lainnya adalah analisis dan korelasi antara insiden untuk mengetahui apa yang belum pernah dilihat sebelumnya (teknik serangan baru, jejak digital, *tools* penyusup, vektor/sumber serangan). Mampu mengidentifikasi aktivitas anomali (atau tidak terduga) tersebut dapat mengarah pada serangan baru atau kerentanan potensial yang memerlukan penyelidikan atau analisis lebih lanjut. Beberapa anggota Tim Tanggap Insiden Siber akan memerlukan keterampilan dan pengetahuan khusus tambahan untuk dapat melakukannya:

- Mengidentifikasi kerentanan baru.
- Melakukan analisis teknis terhadap alat dan teknik penyusup.
- Mengenali teknik intrusi baru berdasarkan jejak digital dan efeknya.
- Mendokumentasikan analisis artefak sebagai bahan referensi untuk anggota tim lain (pekerjaan ini juga dapat diperluas dengan memberikan panduan untuk membantu anggota Tim Tanggap Insiden Siber lainnya mengidentifikasi jejak digital, risiko terkait, dan metode pencegahan).

3) Berkomunikasi dengan situs

Banyak komunikasi yang dilakukan oleh penangan insiden Tim Tanggap Insiden Siber dilakukan secara *online*, biasanya melalui *email*. Korespondensi sering membutuhkan pengiriman data insiden dengan cara yang aman. Akibatnya, penting bagi anggota Tim Tanggap Insiden Siber untuk sepenuhnya fasih dalam penggunaan fungsi *email*, serta *tools* dan metode untuk mengidentifikasi informasi kontak untuk situs lain dan teknologi enkripsi yang sesuai untuk digunakan.

Fungsi dan penggunaan berbagai *tools* untuk memfasilitasi peninjauan dan interpretasi data kejadian juga harus dipahami, seperti format dan *tools* kompresi file, seperti tar UNIX/WinZIP, unicode/decode, dan lainnya. Selain itu, penting untuk memastikan bahwa Anggota Tim Tanggap Insiden Siber mengetahui jenis-jenis koordinasi yang terjadi dalam interaksi antara dan di antara tim-tim lain ini.

4) Analisis insiden

Pada penanganan insiden, Tim Tanggap Insiden Siber berlaku seperti halnya detektif yang menganalisis laporan kejadian, dan mencari jawaban atas pertanyaan seperti berikut ini:

- Siapa yang terlibat?
- Apa yang telah terjadi?
- Dari mana serangan itu berasal?
- Kapan?
- Kenapa ini terjadi?
- Bagaimana sistemnya rentan atau bagaimana serangan itu terjadi?
- Apa alasan/motif serangan itu?

Tim Tanggap Insiden Siber juga perlu mengidentifikasi informasi kritis apa yang hilang, di mana klarifikasi diperlukan, dan efek serta ruang lingkup kegiatan. Tim Tanggap Insiden Siber harus dapat untuk menentukan *tools* atau serangan yang digunakan, tingkat akses yang diperoleh, kerangka waktu, kerusakan atau implikasi yang terkait dengan serangan, dan *host*/ situs yang terlibat.

Anggota Tim Tanggap Insiden Siber juga perlu mengetahui tanggung jawabnya sehubungan dengan tingkat dan kedalaman analisis yang akan dilakukan, bersama dengan pedoman apa pun yang berkaitan dengan pengumpulan data yang sesuai (dari kebijakan operasionalnya sendiri dan/ atau tindakan apa pun yang diambil yang berpotensi mempengaruhi masa depan penggunaan pembuktian atau investigasi hukum).

Anggota Tim Tanggap Insiden Siber harus dapat mengenali pentingnya kegiatan dalam kaitannya dengan prioritas tim, serta menentukan tanggap insiden yang sesuai. Lebih lanjut, Tim Tanggap Insiden Siber perlu menganalisis laporan aktivitas insiden baru untuk menentukan apakah laporan-laporan ini mungkin terkait dengan beberapa cara dengan laporan lain yang ada (*timing* serangan terkait, *signature* dari serangan, kerentanan spesifik yang dieksploitasi, dan lainnya). Dan untuk mengidentifikasi tren atau jenis serupa dari kegiatan yang dapat mempengaruhi konstituennya.

Keahlian dalam bidang analisis insiden mungkin melibatkan analisis mendalam tentang *tools*, *script*, dan artefak lain yang ditemukan selama penanganan insiden dan bahwa anggota Tim Tanggap Insiden Siber lainnya tidak dapat mengidentifikasi. Analisis ini juga dapat mencakup analisis forensik atau pengumpulan data untuk digunakan dalam investigasi kriminal. Bantuan ahli ini mungkin diperlukan untuk menangani eksploitasi dan/atau melakukan tinjauan kode sumber.

5) Pemeliharaan catatan insiden

Peran utama lain dari penangan insiden adalah untuk memelihara catatan insiden. Meskipun keterampilan ini tidak tidak membutuhkan kemampuan khusus, namun keterampilan ini meliputi proses penting yang harus diintegrasikan ke dalam operasi Tim Tanggap Insiden Siber dan diikuti oleh semua anggota tim yang bertanggung jawab atas fungsi penanganan insiden. Untuk memastikan bahwa catatan kejadian dipelihara dengan baik, setiap penangan kejadian Tim Tanggap Insiden Siber harus memahami teknologi yang digunakan untuk memelihara catatan laporan kejadian, informasi pendukung, dan *file* terkait lainnya. Juga sangat penting bahwa catatan kejadian didokumentasikan dengan baik, dipelihara secara konsisten, dan terkini. Memelihara catatan insiden akan memberikan gambaran yang jelas tentang keadaan aktivitas saat ini dan pekerjaan apa yang tersisa. Menyimpan catatan yang baik juga mempermudah koordinasi di antara anggota tim jika perlu untuk menyampaikan laporan kepada pihak lain.

f. Perangkat Pendukung Tim Tanggap Insiden Siber

1) Komunikasi dan fasilitas penanganan insiden
   a) Informasi kontak untuk anggota tim dan orang lain di dalam dan di luar organisasi (kontak utama dan cadangan), seperti lembaga penegak hukum dan Tim Tanggap Insiden Siber lainnya. Informasi kontak dapat mencakup nomor telepon, alamat *email*, kunci enkripsi publik, dan petunjuk untuk memverifikasi identitas kontak.
   b) Informasi panggilan untuk tim lain dalam organisasi, termasuk informasi eskalasi.
   c) Mekanisme pelaporan insiden, seperti nomor telepon, alamat *email*, formulir *online*, dan aplikasi perpesanan (*messaging*) aman yang dapat digunakan pengguna untuk melaporkan dugaan insiden. Setidaknya terdapat 1 (satu) mekanisme harus mengizinkan orang untuk melaporkan insiden secara anonim.
   d) Sistem pelacakan masalah untuk melacak informasi insiden, status, dan lainnya.
   e) *Smartphone* untuk dibawa oleh anggota tim untuk dukungan di luar jam kerja dan komunikasi di tempat.
   f) Perangkat lunak enkripsi yang akan digunakan untuk komunikasi di antara anggota tim, di dalam organisasi dan dengan pihak eksternal.
   g) Ruang perang (*war room*) untuk komunikasi dan koordinasi pusat. Jika ruang perang permanen tidak diperlukan atau praktis, maka Tim Tanggap Insiden Siber harus membuat prosedur untuk mendapatkan ruang perang sementara bila diperlukan.
   h) Fasilitas penyimpanan aman untuk mengamankan bukti dan materi sensitif lainnya.

2) Perangkat keras dan perangkat lunak untuk analisis insiden
   a) *Workstation* untuk forensik digital dan/atau perangkat cadangan untuk membuat *image disk*, menyimpan *file log*, dan menyimpan data insiden relevan lainnya.
   b) Laptop untuk kegiatan seperti menganalisis data, mengendus paket (*packet sniffing*), dan menulis laporan.
   c) Cadangan *workstation*, *server*, dan peralatan jaringan, atau perangkat virtual yang setara, yang dapat digunakan untuk berbagai tujuan, seperti memulihkan cadangan dan mencoba *malware*.
   d) Media penyimpanan portabel (*removable media*) yang kosong.
   e) *Printer* portabel untuk mencetak salinan *file log* dan bukti lain dari sistem yang tidak terhubung ke jaringan.
   f) *Tools* pengendus paket dan penganalisis protokol untuk menangkap dan menganalisis lalu lintas jaringan.
   g) Perangkat lunak forensik digital untuk menganalisis *image disk*.
   h) Media yang dapat dilepas dengan versi program tepercaya yang akan digunakan untuk mengumpulkan bukti dari sistem.
   i) Aksesori pengumpulan bukti, termasuk buku catatan, kamera digital, perekam audio, formulir lacak balak (*chain of custody*), tas dan label penyimpanan bukti, dan pita bukti, untuk menyimpan bukti untuk kemungkinan tindakan hukum.

3) Sumber daya analisis insiden
   a) Daftar *port*, termasuk *port* yang umum digunakan.
   b) Dokumentasi untuk OS, aplikasi, protokol, dan solusi deteksi intrusi dan antivirus.
   c) Diagram jaringan dan daftar aset penting, seperti *server database*.
   d) *Baseline* saat ini dari jaringan, sistem, dan aktivitas aplikasi yang diharapkan.
   e) *Hash* kriptografi dari *file-file* penting untuk mempercepat analisis insiden, verifikasi, dan perbaikan.

4) Perangkat Lunak Mitigasi Insiden

   Image OS yang bersih dan *installer* aplikasi untuk tujuan pemulihan dan pemulihan.

3 - *Malware* Jenis *Worm*

a. Persiapan

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Tentukan personel yang akan terlibat dalam penanganan insiden dan harus didokumentasikan dalam daftar kontak yang terus diperbarui secara permanen.
2) Pastikan *tools* analisis (EDR, antivirus, IDS, *log analyzer*) dalam keadaan aktif, berfungsi dengan baik, tidak disusupi, dan versi ter-*update*.
3) Pastikan terdapat peta arsitektur jaringan.
4) Pastikan terdapat daftar inventaris aset yang terkini.
5) Lakukan pengawasan keamanan terus menerus dan informasikan kepada personel yang bertanggung jawab atas keamanan tentang tren ancaman.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Mendeteksi infeksi, dengan cara mengumpulkan dan menganalisis Informasi yang berasal dari beberapa sumber:
   a) Antivirus *log*.
   b) IDS/IPS.
   c) EDR.
   d) Upaya koneksi yang mencurigakan di *server*.
   e) Banyaknya akun terkunci.
   f) Lalu lintas jaringan yang mencurigakan.
   g) Upaya koneksi yang mencurigakan di *firewall*.
   h) Peningkatan jumlah panggilan telepon ke *customer service* yang signifikan.
   i) Beban yang tinggi pada sistem.
   j) Volume *email* yang dikirim sangat banyak.
2) Jika 1 (satu) atau beberapa dari gejala di atas terlihat, maka personel yang sudah ditentukan dalam daftar kontak di tahap persiapan perlu dihubungi.
3) Identifikasi infeksinya dengan cara menganalisis gejala untuk mengidentifikasi *malware*, vektor penyebarannya, dan penanggulangannya. Sumber informasi dapat berasal dari buletin Tim Tanggap Insiden Siber, kontak pihak eksternal (perusahaan antivirus), situs *web* keamanan, dan penyedia *threat intelligence*.
4) Beri tahu manajemen puncak yang membawahi fungsi teknologi informasi di organisasi.
5) Hubungi Tim Tanggap Insiden Siber dan regulator jika diperlukan.
6) Kaji batas infeksi, yaitu menentukan batas-batas infeksi *malware*.

7) Jika memungkinkan, identifikasi dampak bisnis dari infeksi *malware* tersebut.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Putuskan sambungan area yang terinfeksi dari internet
   a) Isolasi area yang terinfeksi *malware*, putuskan sambungannya dari jaringan apa pun.
   b) Jika lalu lintas bisnis penting tidak dapat diputuskan, sambungkan kembali setelah memastikan bahwa sambungan tersebut tidak dapat menjadi vektor infeksi *malware* atau temukan teknik pengelakan (*circumventions*) yang tervalidasi.
   c) Menetralkan vektor propagasi, dapat berupa apa saja mulai dari lalu lintas jaringan hingga cacat perangkat lunak. Penanggulangan yang relevan harus diterapkan, misalnya tambalan (*patch*), pemblokiran lalu lintas, penonaktifan perangkat.
2) Sebagai contoh, *tools*/teknik berikut dapat digunakan:
   a) EDR.
   b) *Tools* penerapan *patch*, seperti Windows Server Update Services (WSUS).
   c) Windows Group Policy *Object* (GPO).
   d) Aturan *firewall*.
   e) Prosedur operasional.
3) Lakukan pemantauan infeksi *malware* menggunakan *tools* analisis (konsol antivirus, *log server*) untuk memastikan area yang terinfeksi *malware* berhenti menyebar.
4) Pada perangkat *mobile*
   a) Pastikan bahwa tidak ada laptop, *smartphone*, atau media penyimpanan yang dapat digunakan sebagai vektor propagasi oleh *malware*. Jika memungkinkan, blokir semua koneksi *malware*.
   b) Meminta pengguna akhir (*end user*) untuk mengikuti arahan dengan tepat.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden siber di masa depan.

1) Mengidentifikasi *tools* dan metode perbaikan yang dapat digunakan.
2) Sumber daya berikut dapat digunakan:
   a) *Database signature* pada antivirus.
   b) Kontak pihak eksternal.
   c) Situs *web* keamanan.
   d) *Scanning* dengan Yara, Loki, DFIR-ORC, ThorLite.
   e) EDR *search*.

3) Tentukan proses desinfeksi dari *malware* dan harus divalidasi oleh pihak eksternal (misalnya Tim Tanggap Insiden Siber, SOC). Cara paling mudah untuk menyingkirkan *malware* jenis *worm* adalah dengan menginstal ulang aset informasi.
4) Lakukan pengujian, berupa pengujian proses desinfeksi *malware* dan pastikan proses tersebut berfungsi dengan baik tanpa merusak layanan apa pun.
5) Menarapkan *tools* desinfeksi *malware*. Beberapa opsi yang dapat digunakan:
   a) EDR.
   b) Windows WSUS dan GPO.
   c) Penerapan antivirus *signature*.
   d) Desinfeksi *malware* secara manual.
   e) *Patch* kerentanan.
6) Beberapa jenis *worm* dapat memblokir beberapa metode penerapan perbaikan.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Verifikasi semua langkah sebelumnya telah dilakukan dengan benar dan dapatkan persetujuan pihak manajemen sebelum mengikuti langkah selanjutnya.
2) Buka kembali lalu lintas jaringan yang digunakan sebagai metode propagasi oleh *malware*.
3) Sambungkan kembali beberapa area secara bersamaan.
4) Sambungkan kembali laptop dan perangkat *mobile* ke area tersebut.
5) Sambungkan kembali area ke jaringan lokal.
6) Sambungkan kembali area ke internet.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan, yaitu disusun dan disampaikan bagi semua pihak yang relevan. Hal-hal yang harus dijelaskan dalam laporan:
   a) Penyebab awal infeksi *malware*.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan secara salah.
   e) Kerugian finansial akibat insiden.
   f) *Indicator of Compromise* (IoC).
2) Tindakan untuk meningkatkan proses pengelolaan insiden *malware* jenis *worm* harus ditetapkan dengan memanfaatkan pengalaman pada insiden.

4 - Intrusi pada Windows

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Pada perangkat *end user*:
   a) Pastikan bahwa *tools* pemantauan memiliki versi ter-*update*.
   b) Menjalin kontak dengan tim operasi jaringan dan keamanan.
   c) Pastikan bahwa proses pemberitahuan peringatan ditentukan dan diketahui oleh semua personel.
   d) Pastikan semua peralatan di-*setting* pada NTP yang sama.
   e) Pilih jenis file apa yang bisa hilang/dicuri dan batasi akses untuk file rahasia.
   f) Pastikan *tools* analisis aktif, berfungsi (antivirus, EDR, IDS, *log analyzer*), tidak disusupi, dan mutakhir.
   g) Instal aplikasi dari master asli yang sama.
2) Menerapkan solusi EDR pada perangkat *endpoint* dan *server* dengan cara:
   a) *Tools* ini menjadi salah satu landasan tanggap insiden jika terjadi *ransomware* atau insiden skala besar, memfasilitasi tahap identifikasi, penahanan, dan perbaikan.
   b) Jalankan EDR *search* dan *scanning* antivirus dengan aturan eksplisit IoC dan dapatkan indikator pertama untuk melakukan perbaikan.
   c) Tetapkan kebijakan EDR dalam mode *prevention*.
3) Jika EDR tidak ada, akses fisik ke sistem yang mencurigakan harus diberikan kepada penyelidik forensik. Akses fisik lebih disukai daripada akses jarak jauh, karena peretas dapat mendeteksi investigasi yang dilakukan pada sistem, misalnya dengan menggunakan *network sniffer*.
4) Salinan fisik *hard disk* mungkin diperlukan untuk keperluan forensik dan pengumpulan bukti. Terakhir, jika diperlukan, akses fisik mungkin diperlukan untuk memutus sambungan aset informasi yang dicurigai dari jaringan mana pun.
5) Profil akuisisi untuk EDR atau *tools* seperti FastIR, DFIR Orc, KAPE harus disiapkan.
6) Diperlukan pengetahuan yang baik tentang aktivitas jaringan biasa dari aset informasi/*server* sebagai *baseline*. *File* di tempat aman yang menjelaskan aktivitas *port* biasa harus dimiliki untuk membandingkan secara efisien dengan keadaan saat ini.
7) Pengetahuan yang baik tentang layanan biasa yang berjalan di aset informasi bisa sangat membantu. Jangan ragu untuk meminta bantuan dari pakar *cyber security* jika ada. Ide yang bagus juga untuk memiliki peta semua layanan/proses yang sedang berjalan pada aset informasi.

8) Bersiaplah untuk memberi tahu tim *abuse* dan lembaga penegak hukum serta regulator jika diperlukan selama insiden.
9) Dapat menjadi keuntungan nyata di lingkungan organisasi yang besar, apabila semua aset informasi pengguna relatif sama karena dipasang dari *master* yang sama dan terdapat peta semua proses/layanan/aplikasi. Di lingkungan seperti itu, pengguna tidak diizinkan untuk menginstal perangkat lunak, maka proses/layanan/aplikasi tambahan apa pun dapat dipertimbangkan sebagai sesuatu yang mencurigakan.
10) Semakin diketahui bahwa aset informasi dalam keadaan bersih, maka akan semakin besar peluang untuk mendeteksi aktivitas berbahaya yang dijalankan darinya.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

Aktivitas pada tahap identifikasi:

1) Akuisisi bukti
   a) Mengambil data *volatile*
      Warning (data *volatile*): Sebelum melakukan tindakan lainnya, pastikan untuk meng-*capture* memori *volatile* dengan mengunduh dan menjalankan FTK Imager, Winpmem atau utilitas lainnya dari *drive* eksternal. Data *volatile* memberikan informasi forensik yang berharga untuk diperoleh dari data yang sedang berlangsung. Data *volatile* berguna untuk melakukan analisis pada riwayat *command line*, koneksi jaringan, dan lainnya. Gunakan data *volatile* jika memungkinkan.
   b) Mengambil *image* untuk kepentingan triase
      Gunakan *tools* seperti EDR, FastIR, DFIR Orc, KAPE dengan profil yang telah dikonfigurasi sebelumnya. Atau ambil *image* berupa salinan *disk* lengkap dengan *tools* seperti dd, FTKImager, dan lainnya.
   c) *Warning*: Perlu hak akses administrator pada komputer atau *write-blocker* (fisik atau logis) tergantung pada penggunaan.
2) Analisis memori
   a) Carilah proses yang mencurigakan/palsu (*rogue*).
   b) Meninjau proses DLL dan apa yang ditangani.
   c) Periksa artefak jaringan.
   d) Cari injeksi kode (*code injection*).
   e) Periksa keberadaan *rootkit*.
   f) Hapus proses yang mencurigakan untuk analisis lebih lanjut.
3) Jika terdapat masalah dianggap strategis, misalnya mengakses sumber daya yang sensitif, maka prosedur manajemen krisis tertentu harus dijalankan.
4) Identifikasi mekanisme persistensi

Persistensi dapat diizinkan melalui teknik yang berbeda termasuk:

a) *Scheduled task*.
b) Penggantian layanan.
c) Pembuatan layanan.
d) *Auto-start registry keys* dan *startup folder*.
e) Pembajakan pada *order* pencarian DLL.
f) *Library* sistem sah yang dijadikan Trojan.
g) *Local Group Policy*.
h) Microsoft Office *add-in*.
i) Persistensi *pre-boot* (perubahan pada BIOS/UEFI/MBR).

5) Periksa *event logs*
   a) *Log* pada *scheduled tasks* (pembuatan dan eksekusi).
   b) Kejadian akun masuk (periksa koneksi yang berada di luar kantor).
   c) Akun lokal yang mencurigakan.
   d) Layanan berbahaya.
   e) Penghapusan *event logs*.
   f) *Log* RDP/TSE.
   g) *Log* Powershell.
   h) *Log* SMB.
6) *Super-Timeline*
   a) Memproses bukti dan menghasilkan *super-timeline* dengan *tools* seperti Log2timeline;
   b) Analisis *timeline* yang dihasilkan, misalnya dengan TimelineExplorer atau glogg.
7) Untuk melangkah lebih jauh
   a) Pencarian hash.
   b) Anomali MFT dan *timestamping.*
   c) Anti-virus/Analisis Yara/Sigma:
      (1) *Mount* bukti dalam mode *read-only.* Jalankan *scan* antivirus atau beberapa *file* Yara untuk melakukan deteksi cepat.
      (2) Harap perhatikan bahwa *malware* yang tidak dikenal mungkin tidak terdeteksi.
8) Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka prosedur manajemen krisis tertentu harus dijalankan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Pastikan semua vektor serangan telah diidentifikasi sebelum mengambil tindakan penahanan.
2) Mengakuisisi memori dan artefak *volatile* secara selektif.

3) Pilihan tindakan penahanannya yaitu:
    a) Jika aset informasi dianggap penting untuk aktivitas bisnis organisasi dan tidak dapat diputuskan dari jaringan, maka buat pencadangan semua data penting jika peretas mengetahui bahwa aset informasi sedang diselidiki dan *file-file* berbahaya dihapus. Jika memungkinkan, isolasi aset informasi melalui EDR.
    b) Jika aset informasi tidak dianggap kritis untuk organisasi dan dapat diputuskan dari jaringan, maka matikan aset informasi dengan cara yang kasar (*hard way*), yaitu cabut steker listriknya. Jika aset informasi berupa laptop dengan baterai, maka tekan saja tombol *power* selama beberapa detik hingga laptop mati.
4) Investigasi *offline* harus segera dimulai jika analisis langsung tidak memberikan hasil apa pun, tetapi sistem masih harus dianggap disusupi:
    a) Periksa pembagian jaringan atau *folder* apa pun yang dapat diakses publik yang dibagikan dengan pengguna lain untuk melihat apakah terdapat *malware* telah menyebar melaluinya.
    b) Coba temukan bagaimana peretas masuk ke sistem. Semua petunjuk harus dipertimbangkan. Jika tidak ada bukti penyusupan yang ditemukan pada aset informasi, ingatlah bahwa peretas bisa masuk dari akses fisik atau keterlibatan/pencurian informasi dari seorang karyawan.
    c) Terapkan perbaikan pada sistem operasi dan aplikasi, seandainya peretas menggunakan kerentanan yang diketahui.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Peringatan:
    Mulai melakukan perbaikan setelah yakin 100% bahwa perimeter keamanan telah diperbaiki dengan baik untuk mencegah peretas meluncurkan tindakan pembalasan.
2) Jika sistem telah disusupi:
    a) Cara paling mudah untuk menghilangkan *malware* adalah dengan menginstal ulang aset informasi.
    b) Menghapus sementara semua hak akses ke akun yang terlibat dalam insiden tersebut.
    c) Menghapus semua *file* berbahaya yang diinstal dan mekanisme persistensi yang diterapkan oleh peretas.
    d) Terapkan *prevention mode* pada EDR untuk semua IoC yang teridentifikasi.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Tidak peduli seberapa jauh peretas telah masuk ke dalam sistem dan pengetahuan yang diperoleh tentang penyusupan tersebut selama sistem telah dikompromikan, maka praktik terbaiknya adalah menginstal ulang sistem dari media yang asli dan menerapkan semua pembaruan keamanan ke sistem yang baru diinstal.
2) Jika solusi ini tidak dapat diterapkan, maka:
   a) Ubah semua *password* akun sistem dan meminta pengguna untuk melakukannya dengan cara yang aman.
   b) Mengembalikan semua *file* yang mungkin telah diubah oleh peretas, misalnya svchost.exe.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pelaku yang berlaku. Hal-hal berikut harus dibahas:
   a) Deteksi awal.
   b) Tindakan dan *timeline* dari setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Dampak dari insiden tersebut.
   f) *Indicators of compromise* (IoC).
2) Pelajaran yang diperoleh (*lesson learned*)
   a) Tindakan untuk meningkatkan proses manajemen deteksi intrusi Windows harus ditetapkan untuk memanfaatkan pengalaman ini.
   b) Profil *tools* akuisisi dapat di-*tweak* agar lebih cocok dengan artefak yang terdeteksi selama penyelidikan.

5 - Intrusi pada Unix/Linux

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Terapkan solusi EDR pada perangkat *endpoint* dan *server*
   a) *Tools* ini menjadi salah satu landasan tanggap insiden jika terjadi *ransomware* atau kompromi skala besar, memfasilitasi fase identifikasi, penahanan, dan perbaikan.
   b) Lakukan pencarian IoC pada EDR dan *scanning* dengan antivirus untuk melakukan perbaikan.
   c) Tetapkan kebijakan EDR Anda dalam mode *prevention*.
2) Jika tidak ada EDR, maka akses fisik ke sistem yang mencurigakan harus diberikan kepada penyelidik forensik. Proses forensik dengan akses fisik lebih baik daripada akses jarak jauh karena peretas dapat mendeteksi investigasi yang dilakukan pada sistem, misalnya dengan menggunakan *tools network sniffer*.
3) Akses fisik ke sistem yang mencurigakan harus diberikan kepada penyelidik forensik.
4) Salinan fisik *hard disk* diperlukan untuk keperluan forensik dan bukti. Akses fisik diperlukan untuk memutus aset informasi dari sambungan jaringan yang dicurigai.
5) Diperlukan pengetahuan yang baik tentang aktivitas jaringan biasa dari aset informasi. Misalnya *file* di tempat aman yang menjelaskan aktivitas *port* biasa untuk membandingkan secara efisien dengan keadaan saat ini.
6) Diperlukan pengetahuan yang baik tentang layanan biasa. Jangan ragu untuk meminta bantuan dari pakar Unix/Linux, jika ada.
   a) Gunakan Auditd dan Linux *log* seperti *log* sistem, pesan, dan aplikasi (Apache, NGINX)
   b) Gunakan AppArmor, sebagai contoh.
7) Diperlukan daftar semua *file* penting yang diperbarui secara berkala, (terutama file SUID dan GUID) yang disimpan di tempat yang aman di luar jaringan atau bahkan di atas kertas. Dengan adanya daftar ini, maka dapat dengan mudah memisahkan file SUID biasa dan mendeteksi *file* yang tidak biasa.
8) Diperlukan peta dari *usual port activity/traffic rules*.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Akun yang tidak biasa (*unusual accounts*)
   a) Cari entri yang mencurigakan di /etc/passwd, terutama dengan UID 0. Periksa juga /etc/group dan /etc/shadow.

b) Cari *file* tanpa induk, yang mungkin ditinggalkan oleh akun yang dihapus yang digunakan dalam penyerangan:

find / \(--nouser -o --nogroup \) --print

2) *File* yang tidak biasa (*unusual files*)

a) Cari semua *file* SUID dan GUID:

find / -uid 0 \(--perm -4000 -o --perm 2000 \) --print

b) Cari nama *file* yang aneh, dimulai dengan ". " or ".. " or " " :

find / --name " *" –print

find / --name ". *" –print

find / --name ".. *" --print

c) Cari file besar (misalnya lebih besar dari 10 MB):

find / -size +10MB --print

d) Cari proses yang berjalan dari atau ke file yang telah diputuskan tautannya:

lsof +L1

e) Cari *file* yang tidak biasa di /proc dan /tmp. Direktori terakhir ini menjadi tempat pilihan para peretas untuk menyimpan data atau *binary* berbahaya.

3) Layanan tidak biasa (*unusual services*)

a) Jalankan chkconfig (jika diinstal) untuk memeriksa semua layanan yang diaktifkan:

chkconfig --list

b) Lihatlah proses yang sedang berjalan (ingat bahwa *rootkit* mungkin mengubah hasil).

ps –aux

c) Gunakan lsof -p [pid] pada proses yang tidak diketahui

d) Perlu mengetahui proses yang biasa dijalankan dan dapat mengetahui proses mana yang ditambahkan oleh peretas. Berikan perhatian khusus pada proses yang berjalan di bawah UID 0.

4) Aktivitas jaringan yang tidak biasa (*unusual network activity*)

a) Coba deteksi pengendus (*sniffer*) di jaringan menggunakan beberapa cara:

(1) Lihat *file* log kernel untuk antarmuka yang memasuki mode *promiscuous*:

"kernel: device eth0 entered promiscuous mode"

(2) Gunakan link # ip untuk mendeteksi *flag* "PROMISC".

b) Cari aktivitas *port* yang tidak biasa (*unusual port activity*):

netstat -nap

lsof –i

c) Cari entri MAC yang tidak biasa di LAN:

arp -a

d) Cari alamat IP yang tidak terduga atau baru di jaringan:

netstat -ntaupe

netstat -ant

watch ss -tt

5) Tugas otomatis yang tidak biasa (*unusual automated tasks*)

   a) Cari *unusual jobs* yang dijadwalkan oleh pengguna yang disebutkan di /etc/cron.allow. Berikan perhatian khusus pada *cron job* yang dijadwalkan oleh akun UID 0 (root):

      # crontab -u root -l

   b) Cari *cron job* yang tidak biasa (*unusual job*) di seluruh sistem:

      # cat /etc/crontab

      # ls –la /etc/cron.*

6) Entri *Log* yang tidak biasa (*unusual log entries*)

   Lihat melalui *file log* pada sistem untuk kejadian mencurigakan, termasuk berikut ini:

   a) Sejumlah besar kegagalan autentikasi/*login* dari *tools* akses lokal atau jarak jauh (sshd,ftpd).

   b) Program *Remote Procedure Call* (RPC) dengan entri *log* yang menyertakan sejumlah besar karakter aneh.

   c) Sejumlah besar log Apache menyebutkan "*error*".

   d) *Reboot* (*hardware reboot*).

   e) *Restart* aplikasi (*software reboot*).

   f) Catatan

      Hampir semua file *log* terletak di bawah direktori /var/log di sebagian besar distribusi Linux. Namun *path* dapat bervariasi sesuai dengan distribusi Linux):

      - /var/log/message: pesan umum dan hal-hal terkait sistem.
      - /var/log/auth.log: *log* autentikasi.
      - /var/log/kern.log: *log* kernel.
      - /var/log/cron.log: *log* Crond (cron job).
      - /var/log/maillog: log *email server*.
      - /var/log/httpd/: direktori *log* akses dan *error* Apache.
      - /var/log/boot.log: *Log boot* sistem.
      - /var/log/mysqld.log: *File log server database* MySQL.
      - /var/log/secure: *log* autentikasi.
      - /var/log/utmp atau /var/log/wtmp: *file* catatan login.
      - /var/log/syslog: cron, aktivitas samba, dan lainnya.
      - /root/.*history: riwayat perintah pengguna *root*.
      - /home/*/.*history: riwayat perintah pengguna.

   g) Untuk melihat *file log*, *tools* seperti cat dan grep mungkin berguna:

      # cat /var/log/httpd/access.log | grep "GET /signup.jsp

7) Entri *log* Kernel yang tidak biasa (*unusual kernel log entries*)

a) Periksa *file log* kernel pada sistem untuk kejadian yang mencurigakan:

```
# dmesg
```

b) Buat daftar semua informasi kernel dan sistem yang penting:

```
# lsmod
# lspci
```

c) Cari *rootkit* yang dikenal, gunakan rkhunter dan *tools* semacam itu.

8) *File* hash

a) Verifikasi semua *hash* MD5 dari binari di /bin, /sbin, /usr/bin, /usr/sbin atau tempat penyimpanan biner terkait lainnya. Gunakan AIDE atau *tools* semacam itu.

b) *Warning*:
Operasi ini mungkin akan mengubah semua *file timestamp*, sehingga hanya boleh dilakukan setelah semua penyelidikan lain selesai dan dapat mengubah data ini.

c) Pada sistem dengan RPM terpasang, gunakan:

```
# rpm –Va | sort
```

d) Di beberapa Linux, *script* bernama "check-packages" dapat digunakan.

e) Di Solaris:

```
# pkg_chk –vn
```

f) Di Debian:

```
# debsum –ac
```

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Pilihan tindakan penahanannya yaitu:

a) Mencadangkan data penting dengan aman dari aset informasi yang disusupi, jika memungkinkan, menggunakan salinan fisik *bit-by-bit* dari keseluruhan *hard disk* pada sumber eksternal. Buat juga salinan memori (RAM) sistem yang akan diselidiki jika perlu. Kemudian isolasi dengan EDR, periksa komputer dan jaringan lain.

b) Isolasi dengan *firewall* atau *switch*.

2) Catatan
Jika aset informasi tidak dianggap penting bagi perusahaan dan dapat diputuskan sambungannya, maka matikan aset informasi dengan cara yang kasar (*hard way*), yaitu cabut steker listriknya. Jika aset informasi adalah laptop dengan baterai, maka tekan saja tombol *power* selama beberapa detik hingga laptop mati.

3) Investigasi *offline* harus segera dimulai jika langkah identifikasi tidak memberikan hasil apa pun, tetapi sistem masih dicurigai telah disusupi.

4) Cobalah untuk menemukan bukti dari setiap tindakan peretas, misalnya dengan menggunakan *tools* forensik seperti Sleuth Kit/Autopsy:

a) Temukan semua *file* yang digunakan oleh peretas, termasuk *file* yang dihapus dan lihat apa yang telah dilakukan terhadapnya atau setidaknya fungsinya untuk mengevaluasi ancaman.
b) Periksa semua *file* yang diakses baru-baru ini.
c) Periksa *file log*.
d) Coba temukan bagaimana peretas masuk ke sistem. Semua petunjuk harus dipertimbangkan. Jika tidak ada bukti penyusupan pada aset informasi yang ditemukan, maka ingatlah bahwa peretas bisa berasal dari orang dalam (*insider*).
e) Terapkan perbaikan bila berlaku, untuk mencegah jenis intrusi yang sama, seandainya peretas menggunakan kerentanan yang diketahui.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) *Warning*
   Lakukan perbaikan setelah yakin 100% bahwa perimeter keamanan telah dipenuhi dengan baik untuk mencegah peretas meluncurkan tindakan pembalasan.
2) Hapus sementara semua akses untuk akun yang terlibat dalam insiden tersebut dan hapus *file* berbahaya.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Tidak peduli seberapa jauh peretas masuk ke sistem dan pengetahuan yang diketahui tentang peretasan sistem, maka praktik terbaiknya adalah menginstal ulang sistem sepenuhnya dan menerapkan semua perbaikan keamanan.
2) Jika solusi ini tidak dapat diterapkan, maka harus:
   a) Mengubah semua *password* akun sistem dan meminta pengguna melakukannya dengan cara yang aman.
   b) Periksa integritas seluruh data yang disimpan di sistem menggunakan *hash*, misalnya SHA256.
   c) Mengembalikan semua *binary* yang dapat diubah, misalnya: /bin/su.
   d) Mengganti semua paket yang disusupi dengan yang aman.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

Laporan harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan dalam laporan:

a) Deteksi awal.
b) Tindakan dan *timeline*.
c) Apa yang sudah dilakukan dengan benar.
d) Apa yang masih dilakukan dengan salah.
e) Biaya insiden.
f) *Indicators of Compromise* (IoC).

2) Catatan:

Tindakan untuk meningkatkan proses deteksi intrusi Unix/Linux harus ditentukan untuk memanfaatkan pengalaman ini.

6 - DDoS

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Dukungan dari *Internet Service Provider* (ISP)
   a) Hubungi ISP untuk memahami layanan mitigasi DDoS yang ditawarkannya (gratis dan berbayar) dan proses apa yang harus diikuti.
   b) Jika memungkinkan, berlangganlah koneksi internet secara redundan dan berlangganan pada ISP yang anti-DDoS.
   c) Menjalin kontak dengan ISP dan lembaga penegak hukum. Pastikan organisasi memiliki kemungkinan untuk menggunakan saluran komunikasi non-internet, misalnya telepon.
   d) Pastikan ISP dan layanan mitigasi DDoS memiliki dukungan 24/7 melalui telepon.
2) Inventaris
   a) Buat *whitelist* alamat IP dan protokol yang harus diizinkan untuk memprioritaskan lalu lintas selama serangan. Jangan lupa untuk menyertakan daftar pelanggan penting, mitra bisnis utama, dan lainnya.
   b) Dokumentasikan detail infrastruktur TI organisasi, termasuk pemilik bisnis, alamat IP dan ID sirkuit, pengaturan *routing* (AS, dan lainnya), menyiapkan diagram topologi jaringan dan inventarisasi aset.
3) Infrastruktur jaringan
   a) Merancang infrastruktur jaringan yang baik tanpa *Single Point of Failure* atau *bottleneck*.
   b) Menerapkan *Web Application Firewall* (WAF) untuk melindungi dari *application-layer* DDoS.
   c) Distribusikan *server* DNS dan layanan penting lainnya (SMTP, dan lainnya) melalui AS yang berbeda.
   d) Memperkuat konfigurasi komponen jaringan, OS, dan aplikasi yang mungkin menjadi target DDoS.
   e) Buatlah *baseline* kinerja infrastruktur saat ini, sehingga dapat mengidentifikasi serangan dengan lebih cepat dan lebih akurat.
   f) Jika bisnis pada organisasi bergantung pada internet, maka pertimbangkan untuk membeli produk atau layanan mitigasi khusus DDoS.
   g) Konfirmasi pengaturan *time-to-live* (TTL) DNS untuk sistem yang mungkin diserang. Turunkan TTL, jika perlu, untuk memfasilitasi DNS *redirection* jika alamat IP asli diserang. 600 adalah nilai TTL yang bagus.

h) Bergantung pada tingkat kekritisan layanan, pertimbangkan untuk menyiapkan cadangan yang dapat diaktifkan jika terjadi masalah.

4) Kontak internal
   a) Membuatlah daftar kontak yang meliputi IDS, *firewall*, sistem, dan tim jaringan di organisasi.
   b) Berkolaborasi dengan unit kerja bisnis untuk memahami dampak bisnis (misalnya kerugian finansial) dari kemungkinan serangan DDoS.
   c) Libatkan tim yang berperan dalam BCP/DRP pada insiden DDoS.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Periksa latar belakangnya
   a) Cari tahu apakah organisasi menerima upaya pemerasan sebagai pendahulu serangan DDoS
      (1) Periksa *email* di *email gateway* berdasarkan daftar kata kunci (*keyword*).
      (2) Periksa apakah peretas mengirimkan upaya pemerasan langsung ke alamat *email* dalam catatan Whois dari situs *web* yang ditargetkan.
   b) Cari tahu apakah terdapat upaya serangan di media sosial.
   c) Cari tahu apakah ada yang ingin mengancam organisasi:
      (1) Kompetitor.
      (2) Kelompok yang bermotivasi ideologis (peretas).
      (3) Mantan karyawan.
2) Komunikasi
   a) Siapkan *template* komunikasi internal dan eksternal tentang insiden DDoS.
   b) Identifikasi media komunikasi yang akan digunakan.
   c) Fase persiapan harus dianggap sebagai elemen terpenting untuk tanggap insiden DDoS yang berhasil.
3) Analisis serangan
   a) Ingatlah bahwa serangan DDoS bisa menjadi kamuflase untuk menyembunyikan serangan siber lain yang lebih canggih dan terarah.
   b) Periksa analisis layanan anti-DDoS dan laporan dari *scrubbing center*:
      (1) Memahami alur logis dari serangan DDoS dan mengidentifikasi komponen infrastruktur yang terpengaruh olehnya.
      (2) Pahami apakah organisasi adalah target serangan atau korban tambahan.
   c) Meninjau beban dan *file log* dari *server*, *router*, *firewall*, aplikasi, dan infrastruktur lain yang terpengaruh.

d) Identifikasi aspek lalu lintas DDoS apa yang membedakannya dari lalu lintas yang tidak berbahaya
   (1) *Source* alamat IP, AS, dan lainnya.
   (2) Destination ports.
   (3) URL.
   (4) *Protokol flag*.

e) *Tools* analisis jaringan dapat digunakan untuk meninjau lalu lintas jaringan, yaitu: Tcpdump, Tshark, Mendengus, Netflow, Ntop, MRTG, Cacti, Nagios.

f) Jika memungkinkan, buat NIDS *signature* untuk fokus membedakan antara lalu lintas yang tidak berbahaya dan berbahaya.

4) Melibatkan pihak dari internal dan eksternal
   a) Hubungi tim internal organisasi untuk mengetahui tentang visibilitas organisasi dalam serangan tersebut.
   b) Hubungi ISP untuk meminta bantuan yang spesifik tentang lalu lintas yang ingin dikontrol:
      (1) Blok jaringan yang terlibat.
      (2) *Source* alamat IP.
      (3) Protokol.
   c) Beri tahu pihak manajemen dan unit kerja hukum di organisasi.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Jika *bottleneck* adalah fitur tertentu dari aplikasi, maka nonaktifkan sementara fitur tersebut.
2) Mencoba membatasi atau memblokir lalu lintas DDoS sedekat mungkin dengan jaringan publik melalui *router*, *firewall*, *load balancer*, perangkat khusus, dan lainnya.
3) Hentikan koneksi atau proses yang tidak diizinkan pada *server* dan *router*, kemudian sesuaikan pengaturan TCP/IP.
4) Jika memungkinkan, alihkan ke situs atau jaringan alternatif menggunakan DNS atau mekanisme lainnya. Kemudian buatlah lalu lintas *blackhole* DDoS yang menargetkan alamat IP asli.
5) Siapkan saluran komunikasi alternatif antara organisasi dan pengguna/pelanggan, misalnya *server* web, *server email*, *server* VoIP.
6) Jika memungkinkan, *routing*-kan lalu lintas melalui layanan atau produk *traffic-scrubbing* melalui DNS atau perubahan *routing*, misalnya *sinkhole routing*.
7) Konfigurasikan *egress filter* untuk memblokir lalu lintas yang mungkin dikirim oleh sistem sebagai respons terhadap lalu lintas DDoS. Hal ini bertujuan untuk menghindari penambahan paket yang tidak perlu ke jaringan.

8) Jika ada upaya pemerasan, cobalah mengulur waktu. Misalnya, jelaskan bahwa organisasi membutuhkan lebih banyak waktu untuk mendapatkan persetujuan pihak manajemen.
9) Jika *bottleneck* ada di pihak ISP atau layanan anti-DDoS, maka dapat diambil tindakan yang efisien. Organisasi perlu bekerja sama dengan ISP atau penyedia layanan anti-DDoS, serta memastikan organisasi dapat berbagi informasi secara efisien.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghentikan kondisi penolakan layanan.

1) Hubungi ISP dan/atau penyedia anti-DDoS dan pastikan akan dilakukan tindakan perbaikan, dapat berupa:
   a) *Filtering* (jika memungkinkan pada *level* Tier 1 atau 2).
   b) *Traffic-scrubbing/sinkhole/clean-pipe*.
   c) IP *public balancing/splitting/switching*.
   d) Blackhole routing.
2) Tindakan perbaikan teknis sebagian besar dapat dilakukan oleh ISP dan/atau penyedia anti-DDoS.
3) Jika serangan memiliki dampak besar, organisasi harus melaporkan insiden ke regulator.
4) Jika sponsor serangan DDoS telah diidentifikasi, maka dapat dipertimbangkan untuk melakukan penegakan hukum atas arahan pihak manajemen dan unit kerja hukum di organisasi.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Menilai akhir dari kondisi DDoS
   a) Pastikan bahwa layanan yang terpengaruh dapat dijangkau kembali.
   b) Pastikan kinerja infrastruktur kembali ke kinerja dasar (*baseline*).
2) Kembalikan langkah-langkah mitigasi
   a) Mengalihkan kembali lalu lintas ke jaringan asli.
   b) Mulai ulang layanan yang dihentikan.
3) Pastikan bahwa tindakan terkait pemulihan diputuskan sudah dikoordinasikan dengan tim jaringan. Memunculkan layanan dapat memiliki efek samping yang tidak terduga.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dibahas:

   a) Deteksi awal.
   b) Tindakan dan *timeline* dari setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Dampak dari insiden.
   f) *Indicator of Compromise* (IoC).

2) Pelajaran yang diperoleh (*lesson learned*)

   Tindakan untuk meningkatkan proses manajemen DDoS harus ditetapkan untuk memanfaatkan pengalaman ini. Pertimbangkan hubungan di dalam dan di luar organisasi yang dapat membantu organisasi dengan insiden di masa mendatang.

7 - Perilaku Jaringan Berbahaya (*Malicious Network Behaviour*)

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) *Intrusion Detection Systems* (EDR, NIPS, IPS)
   a) Pastikan bahwa *tools* pemantauan sudah *up-to-date*.
   b) Pastikan sudah terjalin kontak antara Tim Tanggap Insiden Siber dengan tim jaringan.
   c) Pastikan bahwa proses pemberitahuan *alert* sudah ditetapkan dan diketahui semua orang.
   d) Verifikasi akses ke perangkat dan kemampuannya untuk mengamati perimeter terkait.
   e) Pastikan dapat dilakukan isolasi pada *endpoint* dan area, misalnya dengan EDR atau *firewall*.
2) Jaringan
   a) Pastikan inventaris *network access point* tersedia, dapat diakses, dan *up-to-date*, jika memungkinkan terdapat versi pembuatan (*versioning*).
   b) Pastikan bahwa tim jaringan memiliki peta dan konfigurasi jaringan terkini terkait zona dan dikoordinasikan dengan tim operasional.
   c) Cari titik akses jaringan potensial yang tidak diinginkan secara teratur dan lakukan penutupan.
   d) Cari akses VPN dan akses *cloud* dari lokasi yang tidak biasa.
   e) Terapkan dan pantau *traffic management tools*.
3) Lalu lintas dasar (*baseline*)
   a) Mengidentifikasi lalu lintas dan arus dasar (*baseline*).
   b) Mengidentifikasi arus bisnis yang bersifat kritis.
4) Catatan
   a) Pastikan Tim Tanggap Insiden Siber merasa nyaman dengan *tools* yang digunakan dan tahu cara menggunakannya.
   b) Tetap operasionalkan *log* meskipun telah diarsipkan.
   c) Memiliki kebijakan retensi *log* yang baik sangat penting (lebih dari 6 bulan).

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Sumber deteksi:
    a) Pemberitahuan oleh pengguna/*helpdesk*.
    b) *Log*, *alert*, dan *report* dari IDS/IPS/NIDS/EDR.
    c) Deteksi oleh staf jaringan.
    d) *Log* pada *firewall* dan *proxy*.
    e) Pengaduan dari pihak eksternal.
    f) *Honeypots* atau teknologi *deceptive* lainnya.
2) Rekam aktivitas jaringan yang dicurigai
    a) *Network frame* dapat disimpan ke dalam *file* dan dikirimkan ke Tim Tanggap Insiden Siber untuk analisis lebih lanjut.
    b) Gunakan *network capture tools* (tshark, windump, tcpdum) untuk membuang lalu lintas berbahaya. Gunakan *hub mirroring* atau *port mirroring* pada LAN yang terpengaruh untuk mengumpulkan data berharga.
    c) Forensik jaringan membutuhkan keterampilan dan pengetahuan. Oleh karena itu, mintalah bantuan atau saran dari Tim Tanggap Insiden Siber.
    d) Ketahui cara memulihkan dan menggunakan dengan *log* meskipun telah diarsipkan.
3) Analisis serangan
    a) Analisis peringatan yang dihasilkan oleh IDS.
    b) Meninjau statistik dan *log* pada perangkat jaringan.
    c) Cobalah untuk memahami tujuan lalu lintas berbahaya dan identifikasi komponen infrastruktur yang terpengaruh olehnya.
    d) Petakan dengan risiko bisnis untuk memprioritaskan analisis atau penahanan dengan benar.
    e) Mengidentifikasi karakteristik teknis lalu lintas:
        (1) *Source* alamat IP.
        (2) *Port* yang digunakan, TTL, Packet ID.
        (3) Protokol yang digunakan.
        (4) Aset informasi/layanan yang ditargetkan.
        (5) *Exploit* yang digunakan.
        (6) Akun jarak jauh yang masuk.
4) Catatan

    Pada akhir langkah ini, aset informasi yang terkena dampak dan modus operandi serangan seharusnya telah diidentifikasi. Idealnya, sumber serangan juga harus diidentifikasi. Pada tahap ini harus melakukan penyelidikan forensik, jika diperlukan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka prosedur manajemen krisis harus diaktifkan. Bergantung pada kekritisan sumber daya yang terkena dampak, langkah-langkah berikut dapat dilakukan dan dipantau:

1) Putuskan sambungan area yang disusupi dari jaringan.
2) Mengisolasi sumber serangan dan putuskan sambungan aset informasi yang terdampak untuk melakukan penyelidikan lebih lanjut.
3) Mengadopsi kontrol mitigasi yang dapat diterima (MFA, *geo-filtering*) untuk proses bisnis kritis sesuai kesepakatan dengan manajer bisnis.
4) Hentikan koneksi atau proses yang tidak diinginkan pada aset informasi yang terdampak.
5) Gunakan aturan *firewall*/IPS/EDR untuk memblokir serangan.
6) Gunakan aturan IDS untuk menyesuaikan dengan perilaku jahat ini dan menginformasikan staf teknis apabila terdapat kejadian baru.
7) Menerapkan tindakan *ad hoc* jika terjadi masalah strategis:
   (1) Tolak *egress destination* pada EDR, proxy, dan/atau *firewall*.
   (2) Mengkonfigurasi *security controls policy management* untuk menahan atau menolak koneksi dari aset informasi yang disusupi.
   (3) Batasi akses ke data penting/rahasia.
   (4) Membuat dokumen jebakan dengan *watermark* yang dapat digunakan sebagai bukti pencurian.
   (5) Beri tahu pengguna bisnis yang ditargetkan tentang apa yang harus dilakukan dan apa yang dilarang.
   (6) Mengonfigurasi kemampuan *logging* dalam mode *verbose* pada lingkungan yang ditargetkan dan menyimpannya di *server* aman secara jarak jauh.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghentikan perilaku berbahaya.

1) Blokir sumbernya
   a) Dengan menggunakan hasil analisis dari langkah-langkah identifikasi dan penahanan sebelumnya, temukan semua saluran komunikasi yang digunakan oleh penyerang dan lakukan pemblokiran di semua *network boundaries*.
   b) Jika sumber telah diidentifikasi sebagai orang dalam (*insider*), ambil tindakan yang tepat dan libatkan pihak manajemen, unit kerja SDM, atau unit kerja hukum.
   c) Jika sumber telah diidentifikasi sebagai pelaku eksternal, pertimbangkan untuk melibatkan unit kerja hukum dan lembaga penegakan hukum jika diperlukan.
2) Perbaikan teknis
   a) Menentukan proses perbaikan. Jika perlu, proses ini dapat divalidasi oleh tim lain, seperti Tim Tanggap Insiden Siber.

b) Dapat menerapkan langkah-langkah perbaikan pada prosedur deteksi intrusi.

3) Uji dan terapkan

a) Menguji proses perbaikan dan memastikannya bekerja dengan baik tanpa merusak layanan apa pun.

b) Terapkan proses perbaikan setelah pengujian disetujui oleh unit kerja TI dan unit kerja bisnis.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Pastikan lalu lintas jaringan sudah kembali normal.

2) Izinkan kembali koneksi ke segmen jaringan yang sebelumnya ada.

3) Catatan:

a) Untuk detail lebih lanjut tentang autentikasi dan pemulihan infrastruktur, periksa Prosedur tentang Insiden Penyusupan/Kompromi Skala Besar.

b) Semua langkah ini harus dilakukan secara bertahap dan dengan pemantauan teknis.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

Sebuah laporan harus ditulis dan tersedia untuk semua aktor. Tema-tema berikut harus dijelaskan:

a) Penyebab awal masalah;

b) Tindakan dan *timeline*;

c) Apa yang dilakukan dengan benar;

d) Apa yang dilakukan dengan salah;

e) Biaya insiden;

f) *Indicator of Compromise* (IoC).

2) Catatan:

Tindakan untuk meningkatkan proses *network intrusion management* harus ditentukan untuk memanfaatkan pengalaman ini.

8 - *Website Defacement*

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Pastikan sudah memiliki skema terkini yang menggambarkan komponen aplikatif yang terkait dengan *server* web.
2) Pastikan sudah memiliki peta jaringan terkini.
3) Membuat situs web cadangan siap pakai yang dapat digunakan untuk mempublikasikan konten.
4) Tetapkan prosedur untuk mengalihkan pengunjung ke situs cadangan ini, misalnya halaman *maintenance* yang statis.
5) Terapkan alat pemantauan dan pencegahan intrusi (WAF, fail2ban, dan sejenisnya) untuk mendeteksi dan mencegah aktivitas abnormal yang menargetkan *server* web yang penting.
6) Mengekspor *file log server* web ke *server* eksternal. Pastikan jam sudah disinkronkan antara setiap *server*.
7) Menerapkan aturan deteksi serangan dan eksploitasi kerentanan berdasarkan *log server* dan memantaunya.
8) Mengaudit situs *web* sebelum dirilis dan secara rutin (setiap bulan jika memungkinkan).
9) Mereferensikan semua sumber konten eksternal yang bersifat statis atau dinamis.
10) Sediakan kontak operasional penyedia *hosting*.
11) Pastikan penyedia *hosting* menerapkan kebijakan untuk mencatat semua kejadian dan memverifikasi kepatuhan kontraktual.
12) Menyiapkan *template* komunikasi jika insiden terlihat oleh pengguna dan perlu dijelaskan.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Saluran deteksi yang biasa adalah:
   a) Pemantauan halaman *web*: Konten halaman *web* telah diubah. Konten baru sangat rahasia (misalnya, injeksi "iframe") atau eksplisit ("... Hacked by xxx").
   b) Pengguna: organisasi menerima panggilan dari pengguna atau pemberitahuan dari karyawan tentang masalah yang ditemukan saat menjelajahi situs web.

c) Pemeriksaan keamanan dengan *tools* seperti Google SafeBrowsing.

2) Verifikasi insiden perusakan dan deteksi asalnya:
   a) Periksa metadata *file* (khususnya, periksa tanggal modifikasi, tanda tangan *hash*).
   b) Periksa penyedia konten *mashup*.
   c) Periksa tautan yang ada dalam kode sumber (src, meta, css, skrip, ...).
   d) Periksa file *log* dan *warning* yang dihasilkan oleh solusi/produk deteksi.
   e) Pindai *database* untuk mencari adanya konten berbahaya.
3) Catatan
   a) Kode sumber laman yang mencurigakan harus dianalisis dengan cermat untuk mengidentifikasi dan memperluas masalah.
   b) Pastikan masalahnya berasal dari *server web* milik organisasi dan bukan dari konten *web* yang terletak di luar infrastruktur organisasi, seperti *banner* iklan dari pihak ketiga.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Cadangkan semua data yang disimpan di *server web* untuk keperluan forensik dan pengumpulan bukti. *Best practice*-nya adalah membuat salinan *bit-to-bit* lengkap dari *harddisk* yang digunakan oleh *server web*. Hal ini dapat membantu untuk memulihkan konten yang dihapus.
2) Periksa peta arsitektur jaringan untuk memerifikasi bahwa tidak terdapat kerentanan lain yang dieksploitasi oleh peretas
   a) Periksa sistem di mana *server web* berjalan.
   b) Periksa layanan lain yang berjalan di *server* tersebut.
   c) Periksa koneksi masuk dan keluar yang dibuat dari *server*.
3) Jika sumber serangan berasal dari sistem lain, maka selidiki sistem yang digunakan.
4) Temukan bukti di balik setiap tindakan yang dilakukan oleh peretas.
5) Cari tahu bagaimana peretas pertama kali masuk ke sistem dan perbaiki penyebab utama
   a) Kerentanan komponen *web* yang memungkinkan akses *write*: perbaiki kerentanan dengan menerapkan perbaikan yang berlaku.
   b) Kerentanan *plugin* CMS sering dimanfaatkan oleh peretas: perlu diidentifikasi dan di-*patch*.
   c) Buka *folder* publik: *folder* dijadikan *private*.
   d) Kelemahan SQL memungkinkan dilakukan injeksi, lakukan perbaiki pada kodenya.
   e) Komponen *mashup*: potong *feed mashup* yang terlibat.
   f) Modifikasi administratif dengan akses fisik: modifikasi hak akses.
6) Catatan

Jika diperlukan, gunakan *server web* sementara yang diperbarui. *Server* harus menawarkan konten yang sama dari salah satu *server web* yang dikompromikan atau setidaknya menampilkan konten yang sah seperti halaman pemeliharaan statis. Yang terbaik adalah menampilkan konten statis sementara, yang hanya berisi kode HTML. Ini mencegah infeksi lain jika peretas masih dapat memanfaatkan kerentanan yang sama.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari *web defacement* di masa depan.

1) Hapus semua konten yang diubah dan ganti dengan konten yang sah, yang dipulihkan dari *backup* sebelumnya.
2) Pastikan konten ini bebas dari kerentanan, lakukan *patch* jika perlu.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Mengubah semua *password* pengguna jika *server* web menyediakan autentikasi pengguna dan terdapat bukti bahwa *password* mungkin telah disusupi. Hal ini memerlukan komunikasi ke pengguna.
2) Jika *server* cadangan telah digunakan, pulihkan komponen *server* web utama ke kondisi normal.
3) Memantau *log* dan *alert* dengan cermat untuk mendeteksi serangan baru.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Komunikasi

   Jika dampak kerusakan telah diketahui oleh publik, maka pertimbangkan untuk menyiapkan dan merilis informasi publik yang menjelaskan insiden tersebut.
2) Laporan

   Laporan harus ditulis dan tersedia untuk semua pihak yang relevan. Topik-topik berikut harus dirinci:
   a) Deteksi awal.
   b) Tindakan dan *timeline*.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.

f) *Indicator of Compromise* (IoC).

g) Jika kerentanan teridentifikasi, maka laporkan setiap kerentanan yang berdampak ke pihak pengembang, sehingga kode dapat ditinjau dan mendapatkan perbaikan resmi.

3) Catatan

Tindakan untuk meningkatkan penanganan insiden *web defacement* harus ditentukan untuk memanfaatkan pengalaman ini.

9 - Deteksi *Malware* pada Windows

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Menerapkan solusi EDR pada *endpoint* dan *server*
   a) *Tools* ini menjadi salah satu landasan tanggap insiden jika terjadi *ransomware* atau insiden skala besar, memfasilitasi fase identifikasi, penahanan, dan perbaikan.
   b) Lakukan EDR *search* dan *scanning* AV pada IoC tertentu dan dapatkan indikator pertama untuk melakukan perbaikan selanjutnya.
   c) Atur EDR dalam mode *prevention* untuk mencegah gangguan bisnis yang tidak perlu.
2) Jika EDR tidak ada, maka akses fisik ke sistem yang mencurigakan harus diberikan kepada penyelidik forensik. Akses fisik lebih disukai daripada akses *remote* karena peretas dapat mendeteksi investigasi yang dilakukan pada sistem, misalnya dengan menggunakan *tools* pelacak jaringan.
3) Salinan fisik *harddisk* mungkin diperlukan untuk keperluan forensik dan bukti. Terakhir, jika diperlukan, akses fisik mungkin diperlukan untuk memutus aset informasi yang dicurigai terdampak dari jaringan mana pun.
4) Profil akuisisi pada EDR atau *tools* akuisisi seperti FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, WinPmem harus disiapkan dan diuji.
5) Diperlukan pengetahuan yang baik tentang aktivitas jaringan biasa dari aset informasi dan dokumentasi yang menjelaskan aktivitas *port* biasa sebagai perbandingan yang efisien dengan keadaan saat terjadi insiden.
6) Pengetahuan yang baik tentang layanan biasa yang berjalan di aset informasi bisa sangat membantu. Jangan ragu untuk meminta bantuan dari pakar Windows, jika ada. Ide yang bagus juga untuk memiliki peta semua layanan/proses di aset informasi yang sedang berjalan.
7) Pastikan bahwa *tools* untuk *monitoring* sudah *up to date*.
8) Terapkan Sysmon, SmartScreen dan terapkan *baseline* rekomendasi dari ANSSI dan CIS.
9) Sudah terjalin kontak antara tim operasi keamanan dengan tim jaringan.
10) Pastikan bahwa proses pemberitahuan *alert* ditetapkan dan diketahui semua orang.
11) Pastikan semua peralatan tersinkronisasi dengan NTP yang sama.
12) Pilih jenis *file* apa yang bisa hilang/dicuri dan batasi akses untuk *file* rahasia.

13) Pastikan alat analisis aktif, berfungsi (AV, EDR, IDS, *log analyzer*), tidak disusupi, dan *up to date*.
14) Instal aplikasi dari *master* asli yang sama.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Catatan

   Rangkaian *malware* yang teridentifikasi akan berdampak pada langkah selanjutnya dari tanggap insiden. Investigasi akan lebih cepat untuk *software* atau *miner* yang tidak diinginkan. *Malware* jenis *stealer, dropper*, atau *ransomware* akan membutuhkan analisis yang lebih dalam dan dapat menyebabkan insiden lainnya.

2) Tanda-tanda umum keberadaan *malware* di *desktop*

   Beberapa petunjuk dapat mengisyaratkan bahwa sistem dapat disusupi oleh *malware*:

   a) EDR, HIDS, aplikasi antivirus memunculkan *alert*, tidak dapat memperbarui *signature*-nya, mematikan atau tidak dapat menjalankan *scanning* manual.
   b) Aktivitas *harddisk* yang tidak biasa: *harddisk* melakukan aktivitas berat pada waktu yang tidak terduga.
   c) Aset informasi menjadi sangat lambat: pelambatan tiba-tiba dan tidak dapat dijelaskan yang tidak terkait dengan penggunaan sistem.
   d) Aktivitas jaringan yang tidak biasa: koneksi internet lambat/kinerja berbagi jaringan buruk dengan interval tidak teratur.
   e) Aset informasi melakukan *reboot* tanpa alasan.
   f) Aplikasi tiba-tiba tidak dapat dijalankan.
   g) Jendela *pop-up* muncul saat *browsing* web, bahkan terkadang bahkan tanpa aktivitas *browsing*.
   h) Alamat IP (jika statis) ada di satu atau beberapa internet *blocklist*.
   i) Pengguna mengeluh tentang adanya kiriman *email* yang bersifat *spam* sementara pengirim *email* tersebut tidak merasa mengirimkannya.

3) Catatan

   Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka prosedur manajemen krisis tertentu harus diaktifkan.

4) Melakukan akuisisi bukti

   a) *Warning* tentang data *volatile*

      Sebelum melakukan tindakan lainnya, pastikan untuk membuat *capture memory volatile* dengan mengunduh dan menjalankan FTK Imager, Winpmem atau utilitas lainnya dari *drive* eksternal. Data *volatile* memberikan informasi forensik yang berharga dan langsung untuk diperoleh.

b) Akuisisi data *volatile* dan ambil *image* untuk triase

   Data *volatile* berguna untuk melakukan analisis pada riwayat *command line*, koneksi jaringan, dan lainnya. Gunakan *volatility* jika memungkinkan. Pada pengambilan *image* untuk triase, gunakan *tools* seperti EDR, FastIR, DFIR Orc, KAPE dengan profil yang telah dikonfigurasi sebelumnya.

c) Ambil *image* dari salinan *disk* lengkap

   Dengan alat seperti dd, FTKImager, dan lainnya.

d) *Warning* tentang *write-blocker*

   Diperlukan hak admin pada aset informasi atau *write-blocker* (fisik atau logis) yang tergantung pada kasus penggunaan.

5) Melakukan analisis memori
   a) Carilah proses yang palsu/menipu (*rogue*).
   b) Meninjau proses dan *handle* dari DLL.
   c) Periksa artefak jaringan.
   d) Carilah kode yang digunakan untuk injeksi.
   e) Periksa keberadaan *rootkit*.
   f) Buang proses yang mencurigakan untuk analisis lebih lanjut.
   g) Catatan

      Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka prosedur manajemen krisis harus dijalankan.

6) Identifikasi mekanisme persistensi

   Persistensi dapat diizinkan melalui teknik yang berbeda termasuk:
   a) *Schedule tasks*.
   b) Penggantian layanan.
   c) Pembuatan layanan.
   d) *Registry key* dan *folder* yang *auto-start*.
   e) Pembajakan pada DLL *search order*.
   f) *Library* sistem sah yang dijadikan Trojan.
   g) *Local Group Policy*.
   h) MS Office Add-in.
   i) Persistensi *pre-boot* (perubahan BIOS/UEFI/MBR).
   j) Catatan

      Dapat menggunakan Microsoft Autoruns untuk mempercepat identifikasi persistensi.

7) Periksa *events log*
   a) *Log* pada *schedule tasks* (pembuatan dan eksekusi).
   b) Kejadian akun *logon* (periksa koneksi yang berasal dari di luar area).
   c) Akun lokal yang mencurigakan.

d) Layanan Berbahaya.
e) Penghapusan *event logs*.
f) *Log* pada RDP/TSE.
g) *Log* pada Powershell.
h) *Log* pada SMB.

8) *Super-timeline*
   a) Memproses bukti dan menghasilkan *super-timeline* dengan *tools* seperti Log2timeline.
   b) Analisis *timeline* yang dihasilkan, misalnya dengan TimelineExplorer atau glogg.

9) Untuk melangkah lebih jauh
   a) Pencarian nilai *hash*.
   b) Anomali MFT dan *timestamp*.
   c) Analisis Anti-virus/Yara/Sigma
      (1) *Mount* bukti dalam mode *read-only*. Jalankan pemindaian anti-virus atau beberapa *file* Yara untuk deteksi cepat.
      (2) Harap perhatikan bahwa *malware* yang tidak dikenal mungkin tidak terdeteksi.

10) Catatan
    Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka prosedur manajemen krisis harus dijalankan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) *Warning* tentang data *volatile*
   Memori dan akuisisi artifak *volatile* selektif harus dilakukan langkah-langkah berikutnya.
2) Jika aset informasi dianggap penting untuk aktivitas bisnis organisasi dan tidak dapat diputuskan, maka buatlah *backup* dari semua data penting. Terutama jika peretas mengetahui bahwa sedang dilakukan penyelidikan dan mulai dilakukan penghapusan *file*.
3) Lakukan isolasi aset informasi melalui EDR, jika memungkinkan. Namun jika aset informasi tidak dianggap kritis untuk organisasi dan dapat terputus, maka matikan aset informasi dengan kasar (*hard way*) yaitu mencabut steker listriknya. Jika aset informasi adalah laptop dengan baterai, maka tekan saja tombol *power* selama beberapa detik hingga laptop mati.
4) Catatan
   Kirim *binary* yang dicurigai ke Tim Tanggap Insiden Siber, atau minta bantuan Tim Tanggap Insiden Siber jika tidak yakin tentang sifat *malware* tersebut. Tim Tanggap

Insiden Siber harus dapat mengisolasi *malware* dan mengirimkannya ke semua penyedia antivirus, termasuk vendor organisasi yang terkait. *Best practise* dalam hal ini adalah membuat *file* zip yang terenkripsi *password* dari *binary* yang mencurigakan.

5) Investigasi *offline* harus segera dimulai jika analisis langsung tidak memberikan hasil apa pun, tetapi aset informasi harus tetap dianggap disusupi
   a) Periksa pembagian jaringan atau *folder* apa pun yang dapat diakses publik yang dibagikan dengan pengguna lain untuk melihat apakah *malware* telah menyebar melaluinya.
   b) Secara umum, coba temukan bagaimana peretas masuk ke sistem. Semua petunjuk harus dipertimbangkan. Jika tidak ada bukti penyusupan yang ditemukan, jangan pernah lupa bahwa hal itu bisa berasal dari akses fisik atau keterlibatan/pencurian informasi dari seorang karyawan.
   c) Terapkan perbaikan jika berlaku (pada sistem operasi dan aplikasi) seandainya peretas menggunakan kerentanan yang diketahui.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) *Warning*

   Lakukan perbaikan setelah 100% yakin bahwa telah dilakukan perbaikan perimeter dengan baik dan mengandung perimeter untuk mencegah peretas meluncurkan tindakan pembalasan.
2) Cara paling mudah untuk menghilangkan *malware* adalah dengan menginstal ulang aset informasi
   a) Hapus *binary* dan *registry entry* yang terkait.
   b) Temukan *best practise* untuk menghapus *malware*. Biasanya dapat ditemukan di situs *web* penyedia antivirus.
   c) Hapus semua *file* berbahaya yang diinstal dan mekanisme persistensi yang diterapkan oleh peretas.
   d) Terapkan mode *prevention* pada EDR untuk semua IoC yang teridentifikasi.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Jika memungkinkan, instal ulang OS dan aplikasi serta pulihkan data pengguna dari *backup* yang bersih dan tepercaya. Jika dianggap perlu, maka dapat dilakukan *reimage* pada *harddisk*.
2) Jika aset informasi belum diinstal ulang sepenuhnya, lakukan hal berikut:

a) Mengembalikan *file* yang mungkin telah dirusak oleh *malware*, terutama *file* pada sistem.
b) Ubah semua *password* akun sistem dan meminta pengguna untuk melakukannya dengan cara yang aman.
c) *Reboot* aset informasi setelah semua *file* yang mencurigakan dihapus dan pastikan bahwa *workstation* tidak menunjukkan perilaku yang tidak biasa. Lakukan *scanning* dengan antivirus dan EDR secara lengkap pada *harddrive* dan memori direkomendasikan.

3) Jika pengguna *end user* merupakan sumber penyusupan, maka kampanye *security awareness* harus diperkuat.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

a) Deteksi awal.
b) Tindakan dan *timeline*.
c) Apa yang sudah dilakukan dengan benar.
d) Apa yang masih dilakukan dengan salah.
e) Biaya insiden.
f) *Indicator of Compromise* (IoC).

2) Catatan

Tindakan untuk meningkatkan proses deteksi dan pemberantasan *malware* harus ditetapkan untuk memanfaatkan pengalaman ini. Profil pada alat akuisisi dapat di-*tweak* agar lebih cocok dengan artefak yang terdeteksi selama penyelidikan.

10 - Pemerasan (*Blackmail*)

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Kontak
   a) Mengidentifikasi kontak internal, seperti Tim Tanggap Insiden Siber, unit kerja hukum, unit kerja komunikasi publik, dan lainnya.
   b) Mengidentifikasi kontak eksternal yang mungkin diperlukan, terutama untuk tujuan investigasi seperti lembaga penegakan hukum.
   c) Pastikan bahwa proses eskalasi insiden sudah ditetapkan, dan para pelakunya ditetapkan dengan jelas.
   d) Pastikan untuk memiliki kemampuan pengumpulan informasi intelijen (berupa komunitas, kontak, dan lainnya) yang mungkin terlibat dalam insiden tersebut.
2) Kesadaran

   Pastikan bahwa semua karyawan terkait mengetahui masalah pemerasan (*blackmail*). Hal ini bisa menjadi bagian dari program *security awareness*.
3) Catatan

   Pastikan proses *backup* dan tanggap insiden sudah ada dan selalu diperbarui.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Siagakan personel yang relevan.
2) Lacak komunikasi apa pun yang terkait dengan insiden tersebut: jangan membuang *email* ke *trash*, catat kontak telepon dengan nomor telepon dan *timestamp* jika ada, faks, dan lainnya. Cobalah untuk mendapatkan sebanyak mungkin detail tentang pengirim, seperti nama, faks, alamat pos, dan lainnya.
3) Periksa kemungkinan tindakan dengan Tim Tanggap Insiden Siber dan unit kerja hukum.
4) Selidiki *email* untuk mendapatkan semua informasi tentang insiden tersebut, seperti nama pengguna, *server* MX, dan lainnya.
5) Jika menyangkut data internal, pastikan terdapat *backup* yang aman dan coba cari tahu bagaimana cara pengumpulannya.
6) Sertakan manajemen puncak untuk memberi tahu bahwa *blackmail* sedang terjadi dan sedang ditangani sesuai dengan proses yang ditentukan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Tentukan bagaimana cara untuk dapat menjawab *blackmail* dan konsekuensi serta dampak jika mengabaikan, menjawab ya atau tidak.
2) Ancaman paling umum yang dikaitkan dengan *blackmail* adalah:
    a) *Denial of Service* (DoS).
    b) Mengungkapkan data sensitif di internet, seperti kartu kredit atau data pribadi lainnya dari pelanggan atau karyawan/direktur internal, data rahasia perusahaan, dan lainnya.
    c) Memblokir akses data dari pengguna, misalnya menghapus data atau mengenkripsi data melalui *ransomware*.
    d) Pengiriman *email* secara massal menggunakan merek tertentu, seperti *spam*, *sextortion*, pornografi pada anak, rumor buruk, dan lainnya.
3) Periksa latar belakangnya
    a) Periksa apakah upaya pemerasan serupa pernah terjadi di masa lalu. Periksa apakah organisasi lain juga mengalami ancaman serupa.
    b) Semua data teknis terkait harus diperiksa dengan hati-hati dan dikumpulkan untuk keperluan investigasi.
    c) Cari tahu apakah ada yang ingin mengancam organisasi:
        (1) Kompetitor.
        (2) Kelompok yang bermotivasi ideologis.
        (3) Mantan karyawan atau karyawan saat ini.
    d) Cobalah untuk mengidentifikasi pelaku dengan informasi yang tersedia.
    e) Lebih umum, coba temukan bagaimana pelaku masuk ke sistem atau mendapatkan objek pemerasan.
4) Hubungi lembaga penegak hukum untuk memberi tahu kejadian ini.
5) Cobalah untuk mendapatkan waktu dan detail dari pelaku dengan menanyakan:
    a) Bukti dari apa yang diklaim: data *sample*, bukti intrusi, dan lainnya;
    b) Batas waktu yang diinginkan oleh pelaku untuk mendapatkan apa yang diinginkan, berupa uang, dan lainnya.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Jika cacat telah diidentifikasi pada aset informasi atau proses yang memungkinkan pelaku mendapatkan akses ke objek pemerasan, maka lakukan perbaikan dengan segera untuk mencegah terjadinya kasus lain.
    a) Setelah mendapatkan informasi sebanyak mungkin, maka abaikan pemerasan dan pastikan pemantauan yang sesuai tersedia untuk mendeteksi dan bereaksi sesuai dengan tindakan yang baru.
    b) Jangan mengambil keputusan remediasi sendirian jika aset atau personel yang strategis menjadi sasaran. Libatkan unit kerja yang sesuai.
2) Ingatlah bahwa jawaban yang bersifat positif untuk pelaku adalah jalan terbuka untuk upaya pemerasan lebih lanjut.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Beri tahu manajemen puncak tentang tindakan dan keputusan yang diambil terkait masalah pemerasan (*blackmail*).

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Jika tidak ingin mengajukan aduan, setidaknya beri tahu lembaga penegak hukum karena organisasi lain mungkin dapat terpengaruh. Pada saat yang sama, beri tahu organisasi lain yang se-hierarki dan di bawah organisasi untuk waspada jika pelaku mencoba melakukan pemerasan serupa.
2) Laporan

   Laporan insiden harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan di dalam laporan:
    a) Deteksi awal.
    b) Tindakan dan *timeline*.
    c) Apa yang sudah dilakukan dengan benar.
    d) Apa yang masih dilakukan dengan salah.
    e) Biaya insiden.
    f) Indicator of Compromise (IoC).
3) Catatan

   Tindakan untuk meningkatkan proses penanganan pemerasan (*blackmail*) harus ditentukan untuk memanfaatkan pengalaman ini.

11 - *Malware* pada *Smartphone*

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) *Helpdesk* untuk perangkat *mobile* harus memiliki proses yang ditentukan jika ada dugaan infeksi *malware*, misalnya ganti *smartphone* pengguna dengan yang baru dan isolasi perangkat yang mencurigakan untuk dianalisis oleh penyelidik forensik.
2) Pengetahuan yang baik tentang aktivitas *smartphone* yang biasa dihargai (*tools* yang *default* dan tambahan yang berjalan di atasnya). Pakar di bidang keamanan *smartphone* dapat membantu penyelidik forensik.
3) Disarankan untuk melakukan hal-hal berikut:
    a) Aktifkan *logging* (MDM, daftar aplikasi atau lainnya).
    b) Instal aplikasi antivirus atau aplikasi keamanan lainnya melalui *smartphone*.
    c) Konfigurasikan VPN untuk menganalisis aktivitas jaringan.
4) Untuk penyelidikan forensik:
    a) Pada Android:
        (1) Aktifkan opsi *developer* dengan USB *Debugging* (perlu hati-hati karena bisa berisiko pada fasilitas publik USB *charging*) atau memiliki proses untuk mengaktifkannya.
        (2) Buka opsi *Original Equipment Manufacturer* (OEM) jika memungkinkan.
    b) Uji hasil ekstraksi terlebih dahulu untuk memastikannya kompatibel dengan bukti.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

Tanda-tanda *smartphone* yang harus dicurigai, antara lain:

1) Aplikasi Antivirus/keamanan memberikan peringatan yang semakin meningkat.
2) Terdapat hak yang diberikan pada aplikasi yang bersifat anomali.
3) Terdapat aktivitas sistem yang tidak normal, fungsi yang berjalan sangat lambat.
4) Aktivitas jaringan yang tidak wajar, koneksi internet yang lambat.
5) Sistem *reboot* atau *shutdown* tanpa alasan.
6) Aplikasi mogok secara tiba-tiba.
7) Pengguna menerima 1 (satu) atau beberapa pesan, berisi karakter yang tidak biasa pada SMS, MMS, pesan Bluetooth, dan lainnya.

8) Peningkatan aktivitas *web*, maka harus dilakukan pemantauan untuk memeriksa aktivitas jaringan yang tidak biasa.
9) Panggilan ke nomor telepon yang tidak dikenal atau pada jam/hari yang tidak biasa.
10) Peningkatan tagihan telepon, maka harus dilakukan pemantauan untuk memeriksa tagihan pengguna yang tidak biasa. Tanyakan kepada pengguna tentang aktivitasnya yang biasa pada *smartphone*, situs *web* yang biasanya dikunjungi, dan aplikasi eksternal apa saja yang dipasang.

c. Penahanan (*Containment*)

Tujuan: mengurangi dampak serangan terhadap lingkungan yang ditargetkan.

1) Minta pengguna untuk memberikan kredensialnya untuk mengakses *smartphone* termasuk:
   a) Kode PIN pada kartu SIM.
   b) *Password* pada *smartphone*.
   c) Kredensial pada iCloud.
   d) Kredensial pada Google Play.
   e) *Backup code*.
2) Akuisisi data
   a) Pastikan pengguna diberikan perangkat *smartphone* pengganti untuk digunakan selama penyelidikan.
   b) Cadangkan data *smartphone* dengan membuat sistem *file* fisik, cadangan logis, atau akuisisi manual.
   c) Masukkan *smartphone* ke dalam tas *faraday,* jika ada.
3) Catatan

   Setelah akuisisi, keluarkan baterai (jika memungkinkan) atau alihkan *smartphone* ke mode *airplane* untuk memblokir semua aktivitas WiFi, Bluetooth, dan lainnya.
4) Tindakan tambahan
   a) Lepas SIM *card* untuk melakukan analisis tambahan di luar *smartphone*.
   b) Lakukan pemindaian dengan aplikasi antivirus atau aplikasi keamanan lainnya terhadap cadangan atau *file* yang diperoleh pada proses forensik.
   c) Lakukan prosedur forensik yang berlaku berdasarkan kasus insiden.
5) Catatan

   Tools khusus harus digunakan oleh tim tanggap insiden untuk melakukan investigasi forensik pada *smartphone*. Gunakan solusi forensik khusus untuk menganalisis data yang diambil atau *smartphone*, seperti Cellebrite, XRY, Oxygen, Axiom, Andriller, dan lainnya.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Hapus ancaman *yang* teridentifikasi pada *smartphone*.
2) Bersihkan *smartphone* yang terinfeksi dan melakukan *hard/soft reset* ke *factory setting* dengan *firmware* yang asli.
3) Masukkan kembali SIM *card* ke *smartphone*.
4) Catatan

   Semua aplikasi berbahaya yang teridentifikasi dan masih tersedia di *marketplace* untuk dihapus.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Instal ulang data dan aplikasi yang disimpan secara selektif dari cadangan.
2) Catatan

   Dapat dipertimbangkan untuk menyimpan perangkat selama periode karantina tambahan untuk melakukan pemeriksaan keamanan yang sesuai.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan insiden harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Deteksi awal.
   b) Tindakan dan *timeline*.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).
2) Catatan

   Tindakan untuk meningkatkan kebijakan keamanan *smartphone* harus ditetapkan untuk memanfaatkan pengalaman ini. Berikan penjelasan mengenai insiden kepada pengguna *end user* untuk meningkatkan *security awareness*-nya.

12 - *Social Engineering*

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, dan mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Meningkatkan *security awareness* pengguna dan kebijakan keamanan.
2) Catatan

   Jangan pernah memberikan data pribadi atau organisasi kepada orang yang tidak dikenal. Ini dapat mencakup ID pengguna, *password*, informasi akun, nama, alamat *email*, nomor telepon (ponsel atau telepon rumah), alamat, NIK, jabatan, informasi tentang *client*, organisasi atau sistem TI. Tujuan dari *social engineering* adalah untuk mencuri sumber daya manusia, rahasia organisasi, atau data pelanggan/pengguna.
3) Laporkan kejadian mencurigakan apa pun kepada atasan yang akan meneruskannya ke manajemen puncak agar pelaporan bersifat terpusat.
   a) Memiliki proses yang ditentukan untuk mengalihkan permintaan aneh apa pun ke "*red phone*", jika diperlukan.
   b) Bersiaplah untuk menangani percakapan dengan pelaku *social enginering* untuk mengidentifikasi informasi mana yang dapat membantu melacak pelaku dan sasarannya.
   c) Periksa unit kerja hukum untuk mengetahui tindakan mana yang diperbolehkan dan reaksi mana yang dapat ditangani oleh unit kerja hukum.
4) *Red phone*:
   a) Nomor telepon *red phone* harus ditandai dengan jelas sebagai *social engineering*.
   b) Nomor telepon pelaku harus mudah diidentifikasi dalam direktori telepon global pada organisasi, namun permintaan untuk menampilkan nomor telepon sebaliknya tidak boleh ditampilkan (tersembunyi).
   c) Saluran *red phone* harus selalu direkam untuk keperluan pengumpulan bukti.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Panggilan telepon dari seseorang yang tidak dikenal kepada pengguna atau kontak layanan organisasi yang meminta informasi terperinci
   a) Jika kontak tersebut bekerja di luar organisasi dan meminta informasi yang mungkin berharga bagi pihak pesaing organisasi, maka tolak permintaannya dan lakukan tahap penahanan (*containment*).

b) Jika kontak tersebut berpura-pura menjadi karyawan organisasi tetapi nomor teleponnya tersembunyi atau bukan nomor internal, maka usulkan opsi agar organisasi akan menelepon kembali ke nomor yang terdapat di direktori organisasi. Jika penelpon setuju, maka hubungi kembali pada nomor yang terdapat di direktori organisasi untuk memeriksa penelpon. Jika penelpon menolak opsi ini, dan lakukan tahap penahanan (*containment*).

c) Catatan

(1) Pelaku *social engineering* mungkin menggunakan beberapa teknik (menimbulkan ketakutan, keingintahuan, empati) untuk membujuk korbannya agar berbicara. Jangan mengungkapkan informasi dalam kondisi apa pun.

(2) Dengarkan baik-baik permintaannya dan pada akhirnya minta nomor telepon untuk dihubungi kembali atau alamat *email* untuk membalas.

(3) Catat dan tetap tenang, meskipun penelpon berteriak atau mengancam, ingatlah bahwa pelaku sedang mencoba menggunakan kelemahan manusia.

d) Jika dapat dilakukan tahap lebih jauh, maka informasi berikut perlu dikumpulkan:

(1) Nama koresponden.

(2) Informasi/orang yang diminta.

(3) Aksen, keterampilan berbahasa.

(4) Gaya bahasa dan pengetahuan mengenai organisasi.

(5) Kebisingan pada latar belakang suara.

(6) Waktu dan durasi panggilan.

2) *Email* dari seseorang yang tidak dikenal yang meminta informasi terperinci:

a) Jika pengirim menggunakan alamat *email* di luar organisasi dan meminta informasi yang mungkin berharga bagi pihak pesaing, maka tolak permintaannya dan lakukan tahap penahanan (*containment*).

b) Jika pengirim menggunakan alamat *email* internal organisasi tetapi meminta informasi aneh, maka tanyakan padanya beberapa penjelasan dan gunakan direktori organisasi untuk mendapatkan nama atasannya yang akan dikirimkan informasi salinannya.

3) Pada akhirnya beri tahu manajemen puncak untuk memberi tahu bahwa telah terjadi insiden yang berkaitan dengan serangan *social engineering* karena mungkin manajemen puncak dapat memahami tujuan serangan sesuai dengan konteksnya.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Pada langkah ini, harus yakin bahwa organisasi sedang berhadapan dengan serangan *social engineering*.

2) Tindakan untuk semua karyawan
    a) Panggilan telepon
        (1) Jika pelaku mendesak karyawan untuk memberikan nomor telepon, ikuti langkah-langkah berikut:
            (a) Gunakan saluran *red phone* pada Tim Tanggap Insiden Siber, jika ada.
            (b) Simpan kontak dengan nomor dengan nama yang ditemukan.
            (c) Segera hubungi tim Tim Tanggap Insiden Siber untuk menjelaskan apa yang terjadi dan nama yang ditemukan.
            (d) Jika pelaku membuat karyawan menjadi terlalu stres dan tidak memberi waktu untuk menemukan nomor *red phone*, maka mintalah pelaku untuk menelepon kembali nanti dan karyawan berpura-pura sedang rapat.
        (2) Jika pelaku ingin menghubungi seseorang, ikuti poin-poin berikut :
            (a) Tempatkan pelaku dan panggil Tim Tanggap Insiden Siber dan jelaskan apa yang terjadi.
            (b) Transfer percakapan pelaku ke Tim Tanggap Insiden Siber (namun jangan berikan nomor dari Tim Tanggap Insiden Siber).
    b) *Email*

    Teruskan ke Tim Tanggap Insiden Siber semua email termasuk header (kirim sebagai dokumen terlampir) untuk tujuan penyelidikan. Mungkin membantu untuk melacak penyerang.
3) Tindakan untuk Tim Tanggap Insiden Siber
    a) Panggilan telepon

    Lanjutkan percakapan dengan penyerang dan gunakan salah satu teknik berikut:
        (1) Meniru identitas orang yang ingin diajak bicara oleh pelaku.
        (2) Perlambat dan akhiri percakapan dan arahkan pelaku untuk membuat kesalahan.
        (3) Jelaskan kepada pelaku bahwa serangan *social engineering* dilarang oleh hukum, berpotensi mendapatkan sanksi dan bahwa tim pengacara akan menangani masalah ini jika terus berlanjut.
        (4) Jika nomor telepon jebakan telah digunakan, bersiaplah untuk menghapusnya, kemudian membuat nomor telepon jebakan yang lain dan ditampilkan di direktori Perusahaan.
    b) *Email*
        (1) Kumpulkan informasi sebanyak mungkin di alamat *email*.
        (2) Analisis *header email* dan coba temukan sumbernya.
        (3) Cari alamat *email* dengan *tools* internet.
        (4) Cari informasi lokasi pengguna yang menggunakan alamat *email*.
        (5) Catatan

Gabungkan semua serangan *social engineering* untuk memvisualisasikan skema.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

Beberapa kemungkinan tindakan perbaikan dapat dicoba:

1) Memberi tahu atau mengajukan pengaduan kepada lembaga penegak hukum.
2) Mendiskusikan masalah bersama pihak-pihak yang bisa dipercaya untuk mengetahui apakah organisasi menghadapi masalah ini sendirian.
3) Mengancam pelaku dengan tindakan hukum jika pelaku dapat diidentifikasi.
4) Laporkan alamat *email* yang digunakan oleh pelaku ke tim *abuse* di penyedia.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Beri tahu manajemen puncak tentang tindakan dan keputusan yang diambil pada kasus *social engineering*.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Beri tahu organisasi yang se-hierarki dan di bawah organisasi tentang insiden tersebut karena hal ini dapat membantu menghindari serangan serupa di kemudian hari.
2) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dijelaskan di dalam laporan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden (kerugian langsung dan tidak langsung).
   f) *Indicator of Compromise* (IoC).
3) Catatan

   Tindakan untuk meningkatkan proses penanganan *social engineering* harus didefinisikan untuk memanfaatkan pengalaman ini, terutama *security awareness*.

13 - Kebocoran Informasi (*Information Leakage*)

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Kontak
   a) Mengidentifikasi kontak teknis internal, seperti Tim Tanggap Insiden Siber, unit kerja komunikasi publik, unit kerja sumber daya manusia dan unit kerja hukum.
   b) Mengidentifikasi kontak eksternal yang mungkin diperlukan, terutama untuk tujuan investigasi, seperti lembaga penegakan hukum.
   c) Menyusun strategi komunikasi untuk pihak internal dan eksternal.
   d) Memiliki kontak ke manajemen puncak.
2) Kebijakan keamanan
   a) Pastikan bahwa informasi tentang nilai-nilai organisasi dijelaskan dalam prosedur, bagan TI, sesi *awareness* dan pelatihan.
   b) Pastikan semua aset berharga diidentifikasi sebagaimana mestinya.
   c) Pastikan bahwa proses eskalasi insiden keamanan ditetapkan, dan pelakunya ditetapkan dan diidentifikasi dengan jelas.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Catatan

   Kebocoran data bisa terjadi dari mana saja. Ingatlah bahwa penyebab kebocoran dapat berupa karyawan individu yang sengaja atau tidak sengaja mem-*bypass* masalah keamanan, atau komputer yang disusupi (seperti *malware*/ransomware).
2) Deteksi masalahnya
   a) Proses pemberitahuan insiden

      Informasi internal dapat menjadi sumber pendeteksian yang baik: informasi dari karyawan, Tim Tanggap Insiden Siber yang mengidentifikasi masalah, dan lainnya.
   b) *Tools monitoring* yang bersifat publik
      (1) Pengamatan pada *search engine* internet dan *database* publik bisa sangat berguna untuk mendeteksi kebocoran informasi.
      (2) Pantau situs *web* daftar *ransomware* untuk mendeteksi potensi kebocoran data termasuk dari pihak ketiga.

c) *Tools* DLP (*Data Loss Prevention*)

Jika ada *tools* DLP di organisasi, maka *tools* ini dapat memberikan informasi yang berharga bagi penanganan insiden kebocoran informasi.

3) Konfirmasi masalah

a) Catatan

Jangan melakukan apapun, tanpa permintaan tertulis dari pihak manajemen yang bertanggung jawab. Berdasarkan nasihat unit kerja hukum, izin tertulis dari pengguna yang terkait mungkin diperlukan.

b) *Email*

(1) Sumber kebocoran data dapat saja mengirimkan data menggunakan alamat *email* organisasi.

(2) Pada sistem *messaging*, cari *email* yang dikirim atau diterima dari akun yang dicurigai atau dengan subjek khusus.

(3) Pada *email client* di *desktop* tersangka penyebab kebocoran data (jika tersedia), gunakan *tools* yang memungkinkan untuk memfilter *email* yang ditandai sebagai *private*. Jika hal ini harus dilakukan, mintalah persetujuan tertulis dari pengguna, atau minta pengguna untuk mendampingi selama dilakukan proses ini.

(4) Jika memungkinkan, lihat *file log* yang terkait.

c) *Browsing*

(1) Data mungkin telah dikirim melalui *email* web/forum/situs *web* tertentu.

(2) Di *server proxy* atau SIEM, periksa *log* yang berkaitan dengan koneksi akun yang dicurigai pada URL yang dicurigai telah digunakan untuk membocorkan data.

(3) Di *desktop* (jika tersedia), periksa *history* pada *browser* yang diinstal. Ingatlah bahwa mungkin terdapat beberapa *browser* berbeda di komputer *desktop* yang sama dan pastikan untuk memeriksa *history* dari setiap *browser*. Jika momen kebocoran data dapat diberi *timestamp*, beberapa *file log* dapat memberikan informasi yang berguna.

d) Perangkat penyimpanan eksternal

(1) Sejumlah perangkat dapat digunakan untuk menyimpan data: USB *keys*, CD-ROM, DVD, *harddisk* eksternal, *smartphone*, kartu memori.

(2) Sedikit informasi yang akan ditemukan mengenai transfer data menggunakan perangkat ini. USB *keys* yang digunakan untuk mentransfer data dapat direferensikan oleh sistem operasi. Analisis forensik dapat mengonfirmasi penggunaan perangkat keras tetapi bukan data yang dikirimkan.

e) File lokal

Jika belum ada yang ditemukan, masih ada kemungkinan untuk menemukan jejak di sistem file lokal tersangka penyebab kebocoran data. Sama seperti untuk penyelidikan pada *email*, gunakan *tools* untuk melakukan *parsing* yang melarang akses apa pun ke zona *private* pengguna. Jika hal ini perlu dilakukan, bertindaklah maka bertindaklah sesuai dengan peraturan perundang-undangan yang berlaku.

f) Pemindahan jaringan
   (1) Beberapa cara dapat digunakan untuk mentransfer data keluar dari perusahaan: FTP, *instant messenger*, dan lainnya. Coba mencari *file log* yang menunjukkan aktivitas tersebut.
   (2) Data mungkin juga dikirim menggunakan VPN atau di *server* SSH. Dalam hal ini, koneksi dapat dibuktikan dengan melihat *file log* tetapi tidak dapat melihat konten yang dikirimkan.

g) *Printer*
   Data dapat dikirim ke *printer* yang terhubung ke jaringan. Dalam hal ini, periksa jejak di *spooler* atau periksa secara langsung di *printer*.

h) *Malware/ransomware*
   (1) Kompromi *malware/ransomware* dapat menjadi sumber kebocoran informasi dan harus ditangani sesuai dengan Prosedur Deteksi *Malware*.
   (2) Bahkan ketika cukup bukti telah ditemukan, selalu cari informasi yang lebih banyak lagi. Jika terbukti bahwa data diperoleh secara curang dari A ke B dengan satu metode, maka mungkin saja data dikirim ke C dengan metode lain. Selain itu, ingatlah bahwa orang lain mungkin dapat mengakses komputer tersebut. Apakah karyawan yang dicurigai benar-benar berada di depan komputer saat kebocoran terjadi?

4) Analisis data terkait jika tersedia
   a) Terkadang, data yang bocor dapat diunduh dan dianalisis oleh Tim Tanggap Insiden Siber. Situs *web* daftar *ransomware* seringkali memberikan informasi yang kebocoran data.
   b) Menggunakan *tools* analisis data seperti Aleph dapat membantu unit kerja hukum memutuskan tindakan apa yang perlu diambil.
   c) Catatan
      Di akhir fase ini, dapat dipertimbangkan untuk melibatkan layanan dari lembaga penegak hukum dan regulator jika diperlukan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Beri tahu pihak manajemen, unit kerja hukum, dan unit kerja komunikasi publik untuk memastikan siap menghadapi insiden kebocoran data yang besar-besaran atau terarah.
2) Bergantung pada sumber kebocoran data, lakukan pemblokiran akses ke URI, *server*, sumber, atau penerima kebocoran data. Tindakan ini harus dilakukan pada semua titik infrastruktur.
3) Melakukan penangguhan (*suspend*) kredensial logis dan fisik pada orang dalam (*insider*) jika kebocoran data telah dikonfirmasi. Libatkan unit kerja SDM dan unit kerja hukum sebelum melakukan tindakan apa pun.
4) Mengisolasi sistem komputasi (*desktop, printer*) yang digunakan untuk membocorkan data guna keperluan analisis forensik. Manipulasi ini harus dilakukan dengan cara yang kasar (*hard way*): cabut steker listrik (dan baterai jika berupa laptop).

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Jika data telah dikirim ke *server* publik, minta pemilik *server* (atau administrator *web*) untuk menghapus data yang dibocorkan. Pastikan untuk menyesuaikan permintaan dengan karakteristik pemilik *web* tersebut, misalnya administrator *web hacktivism* tidak akan bertindak seperti halnya administrator *web* media pers.
2) Jika tidak mungkin menghapus data yang dibocorkan, maka berikan analisis lengkap kepada unit kerja komunikasi publik dan pihak manajemen. Lakukan pemantauan dokumen bocor yang tersebar di situs *web* dan media sosial (Facebook, Twitter, dan lainnya), serta komentar atau reaksi netizen.
3) Berikan informasi kepada unit kerja SDM untuk dapat mengajukan sanksi terhadap orang dalam yang menjadi tersangka sumber kebocoran data.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Jika sistem telah disusupi, maka lakukan pemulihan sepenuhnya.
2) Berikan peringatkan terhadap karyawan atau beberapa tim internal terkait tentang insiden tersebut untuk meningkatkan *security awareness* dan meningkatkan penerapan kebijakan atau prosedur keamanan.
3) Ketika situasi kembali normal, maka saluran komunikasi resmi yang digunakan selama penanganan insiden dapat dihilangkan.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Informasikan organisasi yang se-hierarki dan di bawah oranisasi, serta mitra bisnis untuk berbagi *best practise* untuk diterapkan pada insiden ini untuk menerapkan prosedur serupa di organisasi lain.
2) Laporan

   Laporan insiden harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Dampak insiden.
   f) *Indicator of Compromise* (IoC).
3) Catatan

   Tindakan untuk meningkatkan proses penanganan insiden kebocoran informasi harus ditetapkan untuk memanfaatkan pengalaman ini.

14 - Penyalahgunaan Orang Dalam (*Insider Abuse*)

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Kontak
   a) Pastikan untuk memiliki titik kontak di unit kerja komunikasi publik, unit kerja SDM, dan unit kerja hukum.
   b) Memusatkan *logging* untuk kontrol akses.
   c) Pastikan untuk memiliki proses otorisasi dan mengatur proses penghapusan hak istimewa pada peran pekerjaan sebelumnya.
   d) Memberikan autentikasi yang kuat sesuai dengan risiko aplikasi bisnis.
   e) Menyusun strategi komunikasi internal dan eksternal.
   f) Mempersiapkan proses *Data Loss Prevention* (DLP) sesuai dengan UU Pelindungan Data Pribadi dan unit kerja manajemen risiko.
2) Catatan

   Bersiaplah untuk memberi tahu penyedia yang terlibat dan lembaga penegak hukum serta regulator jika diperlukan selama insiden.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Identifikasi pada aspek teknis
   a) *Alert* dari SIEM atau *tools* yang dapat melakukan korelasi

      Perilaku yang berbahaya dapat dideteksi dengan korelasi beberapa peristiwa yang anomali.
   b) *Alert* dari IDS/IPS yang mendeteksi upaya penyusupan

      Jika orang dalam mencoba meretas sistem, maka hal ini dapat memicu *alert* pada *Intrusion Detection System* (atau *Prevention Detection System*).
   c) *Alert* dari kontrol dan layanan DLP

      Tools dan proses untuk mendeteksi dan mencegah pelanggaran data dan eksfiltrasi data.
   d) *Alert* dari kontrol akses fisik
2) Identifikasi pada faktor manusia
   a) Pihak manajemen

Manajer dari orang dalam mungkin menjadi orang pertama yang menyadari adanya perilaku yang mencurigakan.

b) Kontrol, risiko, dan kepatuhan

Unit kerja tersebut memiliki sistem tersendiri untuk mendeteksi adanya anomali operasional dan dapat memberikan peringatan jika sesuatu yang tidak normal terdeteksi.

c) Kolega

Rekan orang dalam mungkin merupakan saluran pemberitahuan yang paling berharga karena mengetahui dengan baik tentang tugas, proses, dan dampak peran pekerjaannya terhadap organisasi. Sehingga kolega dapat dengan mudah menebak apa yang sedang terjadi di internal organisasi.

d) Pihak eksternal

Mitra atau struktur eksternal juga dapat memiliki kemampuan deteksi secara mandiri. Jika operasi di organisasi telah dipalsukan secara internal, maka entitas eksternal ini dapat memberikan informasi yang mencerahkan.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Catatan

Jangan melakukan apapun tanpa permintaan tertulis dari pihak manajemen yang bertanggung jawab. Berdasarkan nasihat dari unit kerja hukum, izin tertulis dari pengguna terkait mungkin diperlukan.

2) Libatkan personel terkait

Pakar yang relevan harus diberitahu untuk dapat memberikan bantuan. Pemberitahuan ini termasuk kepada pihak manajemen yang membawahi unit kerja SDM, unit kerja hukum, unit kerja komunikasi publik, dan unit kerja bisnis, serta tim teknis yang menangani DLP.

3) Rapat

Seorang manajer SDM harus menemui orang dalam yang dicurigai untuk menjelaskan kepadanya apa yang telah ditemukan dan apa yang akan terjadi. Dukungan dapat diperlukan dari personel dari unit kerja hukum, unit kerja IT dan pihak manajemen.

4) Penurunan hak akses

Jika orang dalam yang dicurigai diizinkan untuk tetap bekerja sampai akhir penyelidikan, berikan dia komputer dengan tingkat otorisasi yang minimum.

5) Pembekuan otorisasi

Menangguhkan (*suspend*) hak akses dan otorisasi orang dalam yang dicurigai yang mencakup izin aplikasi, akun sistem, kunci, dan membuat lencana (*badge*) khusus saat memasuki fasilitas gedung.

6) Akses jarak jauh

   Menangguhkan (*suspend*) kemampuan akses jarak jauh pada *smartphone*, akun VPN, token.

7) Penilaian

   Untuk melakukan penilaian lebih detail, ambil semua perangkat komputasi dari orang dalam yang dicurigai.

8) Kasus 1: aktivitas abnormal

   Jika belum ada tindakan jahat atau penipuan yang terkonfirmasi, maka setidaknya dua penyelidikan harus dimulai sekarang:

   a) Penyelidikan forensik pada perangkat komputer milik orang dalam yang dicurigai.
   b) Investigasi *log* pada komponen jejak audit yang berbeda.

9) Kasus 2: aktivitas jahat/penipuan

   a) Jika aktivitas jahat atau penipuan sudah dikonfirmasi, maka pertimbangkan untuk mengajukan aduan terhadap orang dalam yang dicurigai. Dalam hal ini, jangan mengambil tindakan teknis lebih lanjut. Berikan semua bukti yang diminta kepada unit kerja hukum atau petugas dari lembaga penegak hukum dan siap membantu jika diminta.
   b) Jika terdapat kerusakan akibat insiden penyalahgunaan (*abuse*), pastikan untuk membatasi dampak insiden sebelum mengumumkannya kepada publik. Pastikan untuk memberi tahu pihak berwenang jika diperlukan.
   c) Siapkan rencana komunikasi dengan unit kerja komunikasi publik untuk menyampaikan informasi kepada pelanggan dan mitra bisnis.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

Perbaikan bersifat terbatas jika terjadi insiden penyalahgunaan (*abuse*) oleh orang dalam. Tindakan berikut dapat dipertimbangkan:

1) Mengambil tindakan disipliner terhadap karyawan yang melakukan tindakan jahat (atau memberikan sanksi berupa pemutusan kontrak) dan menghapus semua kredensialnya.
2) Meninjau semua program atau kode *script* yang dibuat oleh orang dalam dan hapus semua kode *script* yang tidak perlu.
3) Meninjau tugas administrator (bagian dari unit kerja TI).
4) Libatkan pihak penyedia yang terlibat dan lembaga penegakan hukum serta regulator jika diperlukan.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Jika insiden tersebut belum dipublikasikan, pastikan untuk memberi tahu semua pemangku kepentingan yang terkena dampak (seperti pelanggan, mitra bisnis) dan otoritas yang diperlukan. Komunikasi ini harus dilakukan oleh manajemen puncak jika terjadi dampak yang sangat besar.
2) Akhirnya peringatkan karyawan tentang masalah ini untuk meningkatkan kesadaran dan memperketat kontrol keamanan.
3) Pulihkan operasi yang telah disalahgunakan oleh orang dalam.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   Beberapa peningkatan mungkin perlu dilakukan mengingat dampak insiden penyalahgunaan orang dalam (*insider abuse*):

   a) Peningkatan proses otorisasi.
   b) Mengontrol peningkatan dalam organisasi.
   c) Kesadaran akan penipuan (*fraud*) dan aktivitas berbahaya yang dapat dilakukan orang dalam.

15 - *Phishing* pada Pelanggan

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Buat daftar semua domain sah milik organisasi. Ini akan membantu menganalisis situasi dan mencegah organisasi untuk memulai prosedur pencopotan (*take down*) pada situs *web* resmi yang terlupakan.
2) Siapkan satu halaman *web* yang di-*hosting* di infrastruktur dan siap dipublikasikan kapan saja, untuk memperingatkan pelanggan tentang serangan *phishing* yang sedang berlangsung. Persiapkan dan uji prosedur penerapannya secara jelas.
3) Siapkan formulir penghapusan *email* yang akan menggunakan untuk setiap kasus *phishing*, jika diperlukan dibuat dalam beberapa bahasa. Ini akan mempercepat proses *take down* yang melibatkan vendor *hosting*.
4) Terapkan DKIM, DMARC, dan SPF pada konfigurasi *email*.
5) Pantau domain *cybersquat* (domain yang memiliki kemiripan nama dengan organisasi) dan konten yang di-*posting* di dalamnya. Kumpulkan informasi mengenai kontak dan penyalahgunaan agar informasi siap digunakan ketika diperlukan.
6) Kontak pihak internal
   a) Menyimpan daftar semua orang yang terlibat dalam pendaftaran nama domain di organisasi.
   b) Menyimpan daftar semua personel yang terakreditasi untuk mengambil keputusan tentang kejahatan siber dan tanggap insiden *phishing*. Jika memungkinkan, buatlah kontrak yang menyebutkan siapa saja personel yang dapat mengambil keputusan.
7) Kontak pihak eksternal
   a) Memiliki beberapa cara untuk dihubungi secara tepat waktu (24/7 jika memungkinkan):
      (1) Alamat *email* yang mudah diingat oleh semua orang, misalnya: keamanan@organisasi.co.id.
      (2) Formulir di situs *web* organisasi dimana lokasi formulir sebaiknya mudah ditemukan, tidak lebih dari 2 klik dari halaman utama.
      (3) Akun Twitter yang publik.
   b) Membuat dan memelihara daftar kontak
      (1) Penyedia *hosting*.
      (2) Penyedia pendaftaran domain (*registry*).
      (3) Penyedia *email*.

c) Buat dan pertahankan kontak di Tim Tanggap Insiden Siber/CSIRT/CERT di seluruh dunia yang mungkin dapat membantu jika diperlukan.

8) Meningkatkan *security awareness* pada pelanggan

Jangan menunggu sampai serangan *phishing* untuk dapat berkomunikasi dengan pelanggan. Tingkatkan *security awareness* tentang serangan *phishing*, jelaskan apa itu *phishing*, dan pastikan pelanggan tahu bahwa organisasi tidak akan pernah meminta kredensial/data pribadi melalui *email* atau telepon.

9) Meningkatkan *security awareness* pada lini bisnis

Para personel di lini bisnis harus menyadari masalah *phishing* dan menganggap keamanan sebagai prioritas. Oleh karena itu, para personel harus menerapkan *best practice* seperti menghindari pengiriman tautan (URL) ke pelanggan dan menggunakan pernyataan resmi yang menyatakan bahwa organisasi tidak akan pernah meminta kredensial/data pribadi secara *online*.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Deteksi *phishing*

a) Pantau semua titik kontak dengan cermat, seperti *email*, formulir *web*, dan lainnya.

b) Terapkan perangkap *spam* dan coba kumpulkan *spam* dari mitra/pihak ketiga.

c) Terapkan pemantauan aktif repositori *phishing*, seperti PhishTank dan Google Safe Browsing.

d) Pantau semua milis khusus yang dapat diakses, atau RSS *feed*/Twitter apa pun yang mungkin melaporkan kasus *phishing*.

e) Gunakan sistem pemantauan otomatis pada semua sumber ini, sehingga setiap deteksi memicu *alarm* untuk reaksi instan.

f) Pantau *log web* organisasi, pastikan tidak ada *referrer* mencurigakan yang membawa pengguna ke situs *web* organisasi. Hal ini sering terjadi ketika situs *web phishing* membawa pengguna ke situs *web* yang sah setelah korban ditipu.

2) Libatkan pihak yang tepat

a) Segera setelah situs *web phishing* terdeteksi, hubungi orang-orang di organisasi yang berwenang untuk mengambil keputusan.

b) Keputusan untuk bertindak atas situs *web*/alamat *email* penipuan harus diambil sesegera mungkin, dalam waktu beberapa menit.

3) Kumpulkan bukti

a) Buat salinan halaman *web phishing* dengan *timestamp*. Gunakan *tools* yang efisien untuk melakukannya, seperti HTTrack. Jangan lupa untuk mengambil

setiap halaman skema *phishing*, jangan hanya halaman yang pertama jika ada beberapa halaman. Jika perlu, ambil *screenshot* pada semua halaman.

b) Periksa kode sumber situs *web phishing*
   (1) Lihat ke mana data diekspor: baik ke konten *web* lain yang tidak dapat diakses (biasanya *script* PHP), dikirim melalui *email* ke alamat *email* pelaku atau menggunakan API aplikasi (seperti Telegram).
   (2) Kumpulkan informasi tentang pelaku *phishing* yang mungkin tersedia di URI, kode sumber, dan sistem pemberian kredensial, seperti alamat *email*, bot Telegram, dan lainnya.
   (3) Apakah gambar/grafik berasal dari salah satu situs *web* resmi, atau disimpan secara lokal?

c) Jika memungkinkan, jika gambar/grafik diambil dari salah satu situs *web* organisasi sendiri, maka gambar/grafik dapat diubah untuk menampilkan logo "situs *web phishing*" di halaman *phishing*.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Sebarkan URL *web phishing*, jika ada
   Gunakan segala cara yang dimiliki untuk menyebarkan URL *phishing* di setiap *browser web*: gunakan opsi Internet Explorer, Chrome, Safari, Firefox, Netcraft *toolbar*, Phishing-Initiative, dll. Hal ini akan mencegah pengguna mengakses situs *web* saat organisasi masih mengerjakan fase perbaikan.
2) Sebarkan konten *email phishing* pada situs *web*/mitra untuk pelaporan *spam*.
3) Berkomunikasi dengan pelanggan
   a) Terapkan halaman *alert*/*warning* dengan informasi tentang serangan *phishing* saat ini.
   b) Jika organisasi terkena dampak beberapa kali dalam seminggu, jangan sering menyebarkan pesan *alerrt*/*warning*, melainkan sediakan halaman informasi *phishing* yang dapat meningkatkan *security awareness*.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghentikan kampanye *phishing*.

1) Jika halaman *phishing* penipuan di-*hosting* di situs *web* yang disusupi, coba hubungi pemilik situs *web* tersebut. Jelaskan dengan jelas *phishing* tersebut kepada pemilik *web*, sehingga dapat diambil tindakan yang tepat berupa menghapus konten *phishing*, dan meningkatkan keamanan di dalam *web*, sehingga pelaku *phishing* tidak dapat kembali menggunakan kerentanan yang sama.

2) Hubungi penyedia *hosting* situs *web* tersebut. Kirimkan *email* ke alamat kontak penyedia *hosting* (umumnya abuse@namapenyediahosting), atau coba hubungi melalui telepon untuk mempercepat.
3) Hubungi penyedia *email* untuk menutup akun penipuan yang menerima kredensial atau data pribadi yang dicuri.
4) Jika ada *redirection* (tautan yang terdapat dalam *email* sering mengarah ke URL *redirection*), hapus juga *redirection* tersebut dengan menghubungi penyedia yang bertanggung jawab atas layanan tersebut.
5) Jika tidak mendapat jawaban, atau tidak ada tindakan yang diambil, maka jangan ragu untuk menelepon kembali dan mengirim *email* secara rutin.
6) Jika proses *take down* terlalu lambat, hubungi Tim Tanggap Insiden Siber/CSIRT/CERT lokal di negara yang terlibat untuk dapat membantu penghapusan konten *phishing*.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Lakukan peniilaian akhir dari kasus *phishing*:

1) Pastikan bahwa halaman dan/atau alamat *email phishing* tidak aktif.
2) Tetap pantau URL *phishing*. Terkadang situs *web phishing* dapat muncul kembali beberapa jam kemudian. Jika *redirection* digunakan dan tidak dihapus, lakukan pemantauan dengan cermat.
3) Di akhir kampanye *anti-phishing*, hapus laman *alert* dari situs *web* organisasi.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   a) Pertimbangkan langkah-langkah persiapan apa yang dapat diambil untuk menanggapi insiden *phishing* dengan lebih cepat atau lebih efisien.

b) Perbarui daftar kontak dan tambahkan catatan tentang cara paling efektif untuk menghubungi setiap pihak yang terlibat.
c) Pertimbangkan hubungan apa di dalam dan di luar organisasi yang dapat membantu penanganan insiden di masa mendatang.
d) Berkolaborasi dengan unit kerja hukum, jika tindakan hukum diperlukan.

16 - Penipuan (*Scam*)

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Buat daftar semua domain sah milik organisasi. Ini akan membantu menganalisis situasi dan mencegah organisasi memulai prosedur *take down* di situs *web* sah yang terlupakan.
2) Siapkan satu halaman *web* yang di-*hosting* di infrastruktur dan siap dipublikasikan kapan saja, untuk memperingatkan pelanggan tentang serangan penipuan (*scam*) yang sedang berlangsung. Persiapkan dan uji juga prosedur penerapan yang jelas.
3) Siapkan formulir *email* penghapusan yang akan digunakan untuk setiap kasus penipuan, jika memungkinkan dibuat dalam beberapa bahasa. Hal ini akan mempercepat saat proses menghubungi penyedia internet selama proses *take down*.
4) Memiliki beberapa cara untuk dihubungi secara tepat waktu (24/7 jika memungkinkan):
   a) Alamat *email* yang mudah diingat, misalnya: keamanan@namaorganisasi.co.id.
   b) Formulir web di situs web organisasi dimana lokasi formulir sebaiknya mudah ditemukan, tidak lebih dari 2 klik dari halaman utama.
   c) Akun Twitter yang publik.
5) Terapkan DKIM, DMARC, dan SPF ke semua konfigurasi *email*.
6) Memelihara kontak
   a) Menyimpan daftar semua personel yang berwenang untuk mengambil keputusan tentang kejahatan siber. Jika memungkinkan, buat kontrak dengan proses yang jelas.
   b) Membuat dan memelihara daftar kontak
      (1) Penyedia *hosting.*
      (2) Penyedia *domain registrar*.
      (3) Penyedia pendaftaran domain (*domain registry*).
      (4) Penyedia *email.*
   c) Buat dan pertahankan kontak di Tim Tanggap Insiden Siber/CSIRT/CERT di seluruh dunia yang mungkin dapat membantu jika dilibatkan.
7) Meningkatkan kesadaran pelanggan

   Jangan menunggu insiden penipuan untuk berkomunikasi dengan pelanggan. Tingkatkan *security awareness* tentang beberapa jenis penipuan, seperti penipuan lotre, penipuan 419 dari Nigeria, dan lainnya, jelaskan penipuan tersebut dan pastikan

pelanggan tahu bahwa organisasi tidak akan pernah menghubungi untuk konfirmasi masalah seperti itu melalui *email*.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Peringatan

   Miliki perangkat khusus untuk mengidentifikasi atau berkomunikasi dengan pelaku penipuan, jangan gunakan perangkat pribadi.

2) Deteksi penipuan

   a) Pantau semua titik kontak dengan cermat, seperti *email*, formulir *web*, dan lainnya.
   b) Pantau domain *cybersquat* dan konten yang di-*posting* di dalamnya. Kumpulkan informasi kontak dan penyalahgunaan untuk disiapkan jika perlu digunakan.
   c) Pantau akun media sosial yang menggunakan identitas dari manajemen puncak atau merek dagang.
   d) Terapkan perangkap *spam* dan coba kumpulkan *spam* dari mitra bisnis atau pihak ketiga.
   e) Terapkan pemantauan aktif repositori *scam*, seperti 419 *scam* (http://aa419.org).
   f) Pantau semua milis khusus yang dapat diakses, atau RSS *feed*/Twitter apa pun, yang mungkin melaporkan upaya *scam*.
   g) Gunakan sistem pemantauan otomatis pada semua sumber tersebut, sehingga setiap pendeteksian dapat memicu *alarm*.

3) Libatkan pihak yang tepat

   a) Segera setelah upaya penipuan terdeteksi, hubungi orang-orang di organisasi yang berwenang untuk mengambil keputusan.
   b) Keputusan untuk bertindak atas alamat *email* palsu harus diambil sesegera mungkin, dalam beberapa menit.

4) Kumpulkan bukti

   Dapatkan contoh *email* penipuan yang dikirim oleh pelaku. Berhati-hatilah untuk mengumpulkan *header email* selain konten *email*. Kumpulkan beberapa *email*, jika memungkinkan, untuk memeriksa alamat IP pengirim yang sebenarnya. Hal ini akan membantu penyelidikan, menganalisis apakah upaya penipuan dikirim dari satu aset informasi atau dari botnet. Jika membutuhkan panduan untuk mengumpulkan *header email*, silakan periksa https://www.spamcop.net/fom-serve/cache/19.html

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Menyebarkan konten *email* penipuan di situs *web*/mitra bisnis/*tools* pelaporan *spam*/penipuan.
2) Berkomunikasi dengan pelanggan mengenai upaya penipuan.
3) Tambahkan URL di *blackhole* DNS, *proxy*, dan daftar blokir *firewall*.
4) Terapkan halaman *alert/warning* dengan informasi tentang upaya penipuan jika merek dari organisasi terpengaruh.
5) Catatan

   Jika organisasi terkena dampak beberapa kali dalam seminggu, jangan selalu menyebarkan pesan *alert/warning* melainkan halaman yang sangat informatif tentang penipuan untuk meningkatkan *security awareness*.

d. Perbaikan (*Containment*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Jika ada halaman *web* palsu yang terkait dengan penipuan tersebut, yang di-*hosting* di situs *web* yang disusupi, maka cobalah menghubungi pemilik situs *web* tersebut. Jelaskan dengan jelas upaya penipuan tersebut kepada pemilik situs *web*, sehingga dapat diambil tindakan yang tepat: menghapus konten penipuan, dan meningkatkan keamanan di dalamnya, sehingga penipu tidak dapat kembali menggunakan kerentanan yang sama.
2) Jika halaman *scam* di-*hosting* di domain *cybersquat*, hubungi juga penyedia *hosting* situs *web* tersebut. Kirim *email* ke alamat kontak penyedia *hosting* (umumnya abuse@namapenyediahosting.co.id) atau coba menghubungi melalui telepon untuk mempercepat.
3) Hubungi penyedia *hosting email* untuk menutup akun palsu pelaku penipuan. Jangan lupa untuk menyertakan salinan *email* penipuan.
4) Hubungi tim *abuse* di media sosial untuk menghapus akun palsu.
5) Blokir pertukaran *email* dengan pelaku penipuan.
6) Jika penyedia tidak memberikan jawaban, atau tidak ada tindakan yang diambil, maka hubungi kembali dan kirim *email* secara teratur.
7) Jika penghapusan terlalu lambat, hubungi Tim Tanggap Insiden Siber/CSIRT/CERT lokal di negara yang terlibat yang dapat membantu menghentikan upaya penipuan, dan jelaskan kesulitan yang dihadapi.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Melakukan penilaian akhir atas kasus penipuan:

1) Pastikan alamat *email* pelaku penipuan telah ditutup.
2) Jika ada situs *web* penipuan yang terkait dengan penipuan tersebut, maka teruslah melakukan pemantauan.
3) Di akhir kampanye anti penipuan, hapus laman *alert/warning* terkait dari situs *web* organisasi.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang sudah dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   a) Pertimbangkan langkah-langkah persiapan apa yang dapat diambil untuk menanggapi insiden penipuan dengan lebih cepat atau lebih efisien.
   b) Perbarui daftar kontak dan tambahkan catatan tentang cara paling efektif untuk menghubungi setiap pihak yang terlibat.
   c) Pertimbangkan hubungan apa di dalam dan di luar organisasi yang dapat membantu penanganan insiden di masa mendatang.
   d) Meningkatkan *filter* DKIM, SPF dan DMARC.
   e) Berkolaborasi dengan unit kerja hukum jika tindakan hukum diperlukan.

17 - Pelanggaran Merek Dagang

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Menyimpan daftar semua merek dagang sah milik organisasi. Hal ini akan membantu dalam menilai situasi yang ada dan mencegah organisasi memulai prosedur pelanggaran pada merek dagang yang sudah usang, atau pelanggaran merek dagang pada situs *web* sah atau akun jejaring sosial yang tidak terkait.
2) Membuat daftar informasi menyeluruh berbasis bukti yang terkait dengan merek dagang organisasi untuk mendukung hak hukum organisasi:
   a) Nama, nama domain yang sah, dan akun media sosial yang digunakan oleh organisasi.
   b) Kata-kata bermerek dagang, simbol, *tagline*, grafik, dan lainnya.
   c) Nomor pendaftaran merek dagang jika berlaku.
   d) Kantor pendaftaran merek dagang dimana merek dagang terdaftar.
   e) Dokumen lain yang menetapkan dengan jelas bahwa merek dagang adalah milik organisasi.
3) Siapkan formulir *email* pelanggaran merek dagang. Hal ini akan membantu mempercepat saat mencoba menjangkau registrar, penyedia layanan, dan pihak terkait lainnya selama prosedur berlangsung.
4) Mempromosikan sistem manajemen domain terpusat menggunakan WHOIS.
5) Mempromosikan iklan *online* yang etis agar tidak muncul dengan nama domain tidak berhak. Mempersiapkan proses dan *template* penghapusan dengan unit kerja hukum.
6) Memiliki proses, pakar, dan teknologi untuk mengelola portofolio merek.
7) Memiliki proses atau penyimpanan terpusat untuk mengelola nama merek, IP, domain, data pribadi, kata kunci, dan lainnya.
8) Kontak pihak internal
   a) Memelihara daftar semua orang yang terlibat dalam pendaftaran merek di organisasi terutama dari unit kerja hukum dan komunikasi publik.
   b) Menyimpan daftar semua orang yang berwenang untuk mengambil keputusan tentang merek dagang dan tindakan pada pelanggaran merek dagang.
9) Kontak pihak eksternal

   Menetapkan dan memelihara daftar kontak eksternal dalam registrar dan penyedia layanan yang terlibat dalam masalah merek dagang.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Deteksi pelanggaran merek dagang, dengan cara
   a) Menyebarkan pemantauan aktif pendaftaran nama domain atau layanan peringatan merek.
   b) Siapkan *feed* untuk memantau nama pengguna, halaman, dan grup di jejaring sosial.
   c) Menganalisis HTTP *referrer* di *log* situs *web* untuk mengidentifikasi unduhan konten palsu dan *mirroring* palsu dari situs *web* organisasi.
   d) Siapkan pemantauan nama merek dengan *search engine* khusus.
   e) Memanfaatkan otomatisasi jika memungkinkan untuk memicu *alarm* dan meningkatkan waktu reaksi.
   f) Kumpulkan dan analisis *alert* dari pihak yang tepercaya.
2) Libatkan pihak yang tepat

   Segera setelah pelanggaran terdeteksi, hubungi orang-orang di organisasi yang berwenang untuk mengambil keputusan.
3) Catatan

   Keputusan untuk bertindak atas nama domain, grup, atau akun pengguna palsu harus diambil sesegera mungkin.
4) Kumpulkan bukti
   a) Kumpulkan bukti pelanggaran nama domain, situs *web*, URL tertentu, halaman, grup, atau detail akun.
   b) Buat salinan dengan *timestamp* dari materi yang melanggar merek organisasi (halaman, grup, blog, forum, *timeline* micro-blogging, dan lainnya) dan ambil *screenshot* jika memungkinkan.

c. Penahanan (*Containment*)

Tujuan: mengurangi dampak pelanggaran terhadap lingkungan yang ditargetkan.

Mengevaluasi dampak pelanggaran merek dagang:

1) Apakah bisa digunakan untuk *traffic redirection* (*cybersquatting, typosquatting*, SEO)?
2) Apakah bisa digunakan untuk *spoofing*, pemalsuan atau *scamming* (*cybersquatting* dengan *redirect* ke website organisasi)?
3) Apakah bisa digunakan untuk memfitnah merek organisasi?
4) Evaluasi visibilitas komponen yang melanggar
   a) Visibilitas situs *web* (peringkat).
   b) Jumlah pengikut di media sosial.

5) Pantau domain yang tidak aktif dan melakukan pelanggaran untuk mengetahui adanya tanda-tanda aktivitas penipuan.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghentikan pelanggaran merek dagang.

1) Dalam sebagian besar masalah merek dagang, pemantauan biasanya sudah cukup. Upaya perbaikan harus dimulai hanya jika terdapat dampak pada organisasi.
2) Nama domain
    a) Hubungi pemilik nama domain dan penyedia layanan *hosting* untuk memberi tahu tentang adanya pelanggaran merek dagang dan meminta bantuan untuk menghapus konten palsu tersebut.
    b) Hubungi registrar nama domain untuk memberi tahu tentang adanya pelanggaran merek dagang dan minta bantuan untuk menonaktifkan nama domain atau mentransfernya kepada organisasi.
    c) Minta pemilik atau registrar nama domain untuk mengalihkan semua permintaan DNS ke *name server* jika memungkinkan.
    d) Jika pemilik nama domain maupun registrar tidak memenuhi permintaan, maka lakukan prosedur penyelesaian sengketa melalui unit kerja hukum.
3) Akun media sosial
    a) Hubungi penyedia layanan dari halaman, grup, atau akun yang melanggar untuk memberi tahu tentang adanya pelanggaran terhadap merek dagang atau pelanggaran persyaratan layanan media sosial dan meminta bantuan untuk menonaktifkan akun yang melakukan pelanggaran.
    b) Meminta penyedia layanan untuk mentransfer akun bermerek dagang ke akun organisasi yang sudah ada jika memungkinkan.
4) Catatan
    a) Dalam kasus tersebut, kirim *email* ke alamat kontak registrar atau penyedia layanan. Biasanya ada alamat *email* untuk melaporkan masalah penyalahgunaan, hukum, atau hak cipta.
    b) Isi formulir keluhan merek dagang atau penyalahgunaan jika tersedia.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Menilai akhir dari kasus pelanggaran

1) Pastikan bahwa nama domain, halaman, grup, atau akun yang melanggar di-*take down* atau dialihkan ke organisasi.

2) Pantau terus nama domain, halaman, grup, atau akun yang melakukan pelanggaran. Terkadang sebuah situs *web* dapat muncul kembali nanti.
3) Pertimbangkan untuk mendapatkan nama domain yang melanggar jika tersedia.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: medokumen detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan.

1) Laporan

   Laporan harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang sudah dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   a) Pertimbangkan langkah-langkah persiapan apa yang dapat diambil untuk menanggapi insiden pelanggaran merek dagang dengan lebih cepat atau lebih efisien.
   b) Perbarui daftar kontak dan tambahkan catatan tentang cara paling efektif untuk menghubungi setiap pihak yang terlibat.
   c) Pertimbangkan hubungan apa di dalam dan di luar organisasi yang dapat membantu penanganan insiden di masa mendatang.
   d) Berkolaborasi dengan unit kerja hukum jika tindakan hukum diperlukan.

18 - *Phishing*

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Siapkan komunikasi, siap dipublikasikan kapan saja, untuk memperingatkan pihak yang terkait di organisasi tentang serangan *phishing* yang sedang berlangsung. Persiapkan dan uji juga prosedur penerapan yang jelas.
2) Terapkan DKIM, DMARC, dan SPF ke semua konfigurasi *email*.
3) Menerapkan mekanisme *multi factor authentication* (MFA).
4) Pantau domain *cybersquat* dan konten yang di-*posting* di dalamnya. Kumpulkan informasi kontak dan penyalahgunaan untuk siap digunakan jika diperlukan.
5) Kontak pihak internal
   a) Menyimpan daftar semua orang yang terlibat dalam pendaftaran nama domain di organisasi.
   b) Menyimpan daftar semua orang yang berwenang untuk mengambil keputusan tentang kejahatan siber dan tindakan terkait *phishing*.
6) Kontak pihak eksternal
   a) Memiliki beberapa cara untuk dihubungi secara tepat waktu (24/7 jika memungkinkan):
      (1) Alamat *email*, mudah diingat, misalnya: keamanan@namaorganisasi.co.id.
      (2) Formulir web di situs web organisasi dengan lokasi formulir yang mudah ditemukan, tidak lebih dari 2 klik dari halaman utama.
      (3) Akun Twitter yang publik.
   b) Membuat dan memelihara daftar kontak
      (1) Penyedia *hosting.*
      (2) Penyedia pendaftaran (*registry*).
      (3) Penyedia *email*.
   c) Buat dan pertahankan kontak di Tim Tanggap Insiden Siber/CSIRT/CERT di seluruh dunia yang mungkin dapat membantu jika diperlukan.
   d) Meningkatkan kesadaran pelanggan

      Jangan menunggu sampai *phishing* dapat berkomunikasi dengan pelanggan. Tingkatkan kesadaran tentang *phishing*, jelaskan apa itu *phishing*, dan pastikan pelanggan tahu bahwa organisasi tidak akan pernah meminta kredensial/informasi perbankan melalui *email* atau telepon.
   e) Meningkatkan *security awareness* pada lini bisnis

(1) Personel di lini bisnis harus menyadari masalah *phishing* dan menganggap keamanan sebagai prioritas. Oleh karena itu, mereka harus menerapkan *best practise* seperti menghindari pengiriman tautan (URL) ke pelanggan dan menggunakan pernyataan bertanda tangan yang menyatakan bahwa organisasi tidak akan pernah meminta kredensial/informasi secara *online*.
(2) Jalankan kampanye kesadaran *phishing* secara berkala.
(3) Terapkan solusi teknis yang memungkinkan pihak lain dengan mudah melaporkan *email* ke tim keamanan di organisasi.
(4) Menetapkan prosedur khusus untuk lampiran dan analisis URL.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Deteksi *Phishing*
   a) Pantau semua titik kontak dengan cermat, seperti *email*, formulir *web*, dan lainnya.
   b) Terapkan jebakan *spam* dan coba kumpulkan *spam* dari mitra bisnis/pihak ketiga.
   c) Terapkan pemantauan aktif repositori *phishing*, seperti PhishTank dan Google Safe Browsing.
   d) Pantau semua milis khusus yang dapat diakses, atau RSS *feed*/Twitter yang mungkin melaporkan kasus *phishing*.
   e) Gunakan sistem pemantauan otomatis pada semua sumber ini, sehingga setiap deteksi memicu *alarm* untuk cepat tanggap.
   f) Pantau log *web* organisasi untuk memastikan tidak ada *referrer* mencurigakan yang membawa pengguna ke situs *web* organisasi. Hal ini sering terjadi ketika situs *web phishing* membawa pengguna ke situs *web* yang sah setelah pengguna ditipu.
2) Cakupan serangan *phishing*
   a) Menentukan jumlah pengguna yang ditargetkan.
   b) Cari akun yang telah disusupi yang dieksploitasi dan identifikasi aktivitas jahat terkait.
3) Analisis *phishing*

   Ingatlah untuk mengikuti prosedur analisis yang telah ditetapkan
   a) Tentukan hal berikut:
      (1) Apakah termasuk kampanye pengambilan kredensial atau kampanye penyebaran *malware*?
      (2) Apakah kampanye tersebut merupakan serangan yang ditargetkan atau tidak?

b) Periksa subjek dan isi pesan.
c) Gunakan lingkungan *sandbox* untuk menganalisis *attachment* berbahaya dan mengekstrak IoC.
d) Menganalisis tautan, domain, dan nama *host* dengan layanan *threat intelligence*.
e) Periksa kode sumber situs *web phishing*.
f) Selidiki *header email* untuk mencari artefak yang berelasi, misalnya informasi *server* dan pengirim asal.

4) Kumpulkan bukti

Buat salinan halaman *web phishing* dengan *timestamp*. Gunakan *tools* yang efisien untuk melakukannya, seperti HTTrack. Jangan lupa untuk mengambil setiap halaman skema *phishing*, jangan hanya yang pertama jika ada beberapa. Jika perlu, ambil *screenshot* halaman.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Memblokir IoC jaringan yang ditemukan melalui lampiran/analisis URL pada DNS, *firewall*, atau *proxy*.
2) Memblokir kampanye *phishing* berdasarkan pengirim, subjek, atau artefak *email* lainnya melalui *gateway email*.
3) Coba hapus *email phishing* dari kotak masuk (*inbox*).
4) Terapkan DNS *Sinkhole* pada URL yang mencurigakan (opsional tergantung pada arsitektur DNS).
5) Berkomunikasi dengan semua pihak yang relevan.
6) Terapkan halaman *alert/warning* dengan informasi tentang serangan *phishing* yang terjadi.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghentikan kampanye *phishing*.

1) Mengubah dan/atau memblokir kredensial masuk sementara dari akun yang disusupi.
2) Jika kampanye *phishing* ditargetkan, pertimbangkan untuk menghubungi lembaga penegak hukum, regulator, dan Tim Tanggap Insiden Siber yang relevan.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

Nilai akhir dari kasus *phishing*

1) Pastikan bahwa halaman dan/atau alamat *email* penipuan tidak aktif.

2) Tetap pantau URL penipuan. Terkadang situs *web phishing* dapat muncul kembali beberapa jam kemudian. Jika *redirection* digunakan dan tidak dihapus, pantau dengan cermat.
3) Di akhir kampanye *anti phishing*, hapus halaman *alert* terkait dari situs web organisasi.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan harus ditulis dan tersedia bagi semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   a) Pertimbangkan langkah-langkah persiapan apa yang dapat diambil untuk menanggapi insiden tersebut dengan lebih cepat atau lebih efisien.
   b) Perbarui daftar kontak dan tambahkan catatan tentang cara paling efektif untuk menghubungi setiap pihak yang terlibat.
   c) Pertimbangkan hubungan apa di dalam dan di luar organisasi yang dapat membantu penanganan insiden di masa mendatang.
   d) Berkolaborasi dengan unit kerja hukum jika tindakan hukum diperlukan.

19 - *Ransomware*

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Pengetahuan yang baik tentang hal-hal berikut:
   a) Kebijakan keamanan pada sistem operasi.
   b) Kebijakan profil untuk pengguna *end user*.
   c) Pada arsitektur, segmentasi VLAN dan interkoneksi diperlukan kemampuan untuk mengisolasi entitas, wilayah, mitra bisnis, atau internet.
2) Pastikan bahwa produk keamanan *endpoint* dan perimetrik, seperti *email gateway, proxy cache*, adalah yang ter-*update*.
3) Terapkan solusi EDR pada perangkat *endpoint* dan *server*
   a) *Tools* ini menjadi salah satu landasan tanggap insiden jika terjadi *ransomware* atau dalam kompromi skala besar, memfasilitasi fase identifikasi, penahanan, dan perbaikan.
   b) Lakukan EDR *search* dan *scanning* antivirus dengan IoC untuk dapatkan indikator yang bermanfaat dalam melakukan perbaikan.
   c) Tetapkan kebijakan EDR dalam mode *prevention*.
4) Karena ancaman ini sering terdeteksi oleh pengguna *endpoint*, tingkatkan kesadaran dukungan TI terkait ancaman *ransomware*.
5) Blokir IoC yang terkait dengan aktivitas *ransomware* yang dikumpulkan oleh *threat intelligence*.
6) Menyebarkan dan mengoperasikan solusi keamanan yang memungkinkan deteksi dan memfasilitasi tanggap insiden
   a) Pengumpulan *log* dalam SIEM.
   b) Memiliki kapasitas untuk menjalankan *tools* seperti YARA atau DFIR-ORC (ANSSI).
7) Miliki retensi dan verbositas *log* yang baik.
8) Tentukan postur keamanan yang ketat dari sudut pandang penyerang (*attacker*).
9) Menyiapkan strategi komunikasi internal dan eksternal.
10) Jika aset informasi teridentifikasi terkena *ransomware*, maka cabut dari jaringan dan tetap hidupkan untuk penyelidikan forensik pada memori.
11) Persiapankan *backup*
   a) Pastikan untuk memiliki *backup* data pengguna lokal dan jaringan yang lengkap, terkini, dan andal.
   b) Dapat mengikuti aturan *backup* 3-2-1 untuk memastikan bahwa data disimpan dengan berbagai cara. Jadi, ketika mem-*backup* sesuatu, akan dimiliki:

(1) Setidaknya 3 (tiga) salinan yang berbeda di tempat berbeda. Dengan mempertahankannya tempat yang berbeda, ini mengurangi risiko 1 (satu) peristiwa menghancurkan banyak salinan.

(2) Dalam 2 (dua) format berbeda, yaitu menggunakan setidaknya 2 (dua) metode berbeda untuk menyimpan data. Misalnya, DVD, *harddrive*, layanan *cloud* adalah format yang berbeda. Namun jika menyimpan 2 (dua) salinan ke dalam 2 (dua) *harddrive*, maka artinya hanya digunakan 1 (satu) format.

(3) Dengan salah satu salinan tersebut di luar kantor: Menyimpan 1 (satu) salinan di luar situs memastikan bahwa apa pun yang terjadi di tempat data berada, seperti kebakaran, pembobolan, bencana alam, maka setidaknya 1 (satu) salinan aman di tempat lain. Dalam aturan ini, layanan *cloud* bisa diterapkan.

c) Coba gunakan 1 (satu) format cadangan yang disimpan di luar jaringan: bahkan pergerakan lateral yang terjadi dari ancaman yang membahayakan jaringan dengan enkripsi, 1 (satu) salinan tidak akan dapat dijangkau.

b. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Membuat pernyataan publik sesegera mungkin berdasarkan *template* komunikasi yang diuraikan pada tahap persiapan.
2) Ikuti postur yang ditentukan dalam fase persiapan.
3) Kirim sampel yang tidak terdeteksi ke penyedia keamanan *endpoint* dan/atau *sandbox* pribadi.
4) Kirim URL berbahaya yang tidak dikategorikan, nama domain, dan IP ke penyedia keamanan perimetrik organisasi.
5) Blokir lalu lintas ke C2.
6) Blokir IP apa pun yang terdeteksi digunakan oleh penyerang.
7) Isolasi VLAN, interkoneksi, entitas, wilayah, mitra, atau internet yang disusupi.
8) Nonaktifkan akun yang disusupi/dibuat oleh pelaku.
9) Putuskan sambungan semua komputer yang telah terdeteksi sebagai disusupi dari jaringan. Isolasi dapat dilakukan dengan EDR, mematikan internet dengan hanya mempertahankan koneksi EDR.
10) Jika tidak dapat mengisolasi komputer, putuskan *shared drive*. (NET USE x: \\unc\path\ / DELETE)
11) Pantau situs *web* pelaku ancaman *ransomware* dan internet untuk mengetahui apakah ada publikasi kebocoran data yang terkait dengan penyusupan *ransomware*.

c. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Hapus akses awal yang digunakan oleh penyerang.
2) Hapus *binary* yang digunakan oleh penyerang untuk melakukan lateralisasi pada jaringan.
3) Hapus semua akun yang dibuat oleh penyerang.
4) Kembali perubahan konfigurasi.
5) Mengoperasikan *hardening* pada konfigurasi sistem dan jaringan.

d. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal

1) Perbarui antivirus *signature* agar *binary* berbahaya yang teridentifikasi dapat diblokir.
2) Pastikan tidak ada *binary* berbahaya di sistem sebelum menyambungkannya kembali.
3) Pastikan lalu lintas jaringan sudah kembali normal.
4) Pulihkan dokumen pengguna dari cadangan. Prioritaskan rencana pemulihan berdasarkan *Disaster Recovery Plan* (DRP).
5) Semua langkah ini harus dilakukan secara bertahap dan dengan pemantauan teknis
   a) Pastikan *backup* tidak terganggu: hanya pulihkan dari *backup* jika sangat yakin bahwa *backup* dan perangkat yang disambungkan bersih dari *ransomware*.
   b) Jika tidak, maka lakukan hal berikut:
      (1) Instal ulang aset informasi dengan instalasi yang bersih.
      (2) Atur ulang kredensial termasuk *password* (terutama untuk administrator dan akun sistem lainnya).
6) Pantau lalu lintas jaringan untuk mengidentifikasi apakah masih terdapat infeksi.
7) Jika memungkinkan, terapkan *geo-filtering* pada *firewall* untuk memblokir lalu lintas dari luar negeri yang tidak sah.
8) Pertahankan pemantauan situs *web* aktor ancaman *ransomware* dan internet untuk menemukan apakah ada publikasi kebocoran data yang terkait dengan kompromi *ransomware*.

e. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

a) Penyebab awal infeksi.
b) Tindakan dan *timeline* setiap peristiwa penting.
c) Apa yang sudah dilakukan dengan benar.
d) Apa yang sudah dilakukan dengan salah.
e) Biaya insiden.
f) *Indicator of Compromise* (IoC).

2) Catatan

Tindakan untuk meningkatkan pertahanan terhadap *malware* dan proses deteksi intrusi di jaringan harus ditentukan untuk memanfaatkan pengalaman ini.

20 - Penyusupan/Kompromi Skala Besar

a. Persiapan

Tujuan: membangun kontak, menentukan prosedur, mengumpulkan informasi untuk menghemat waktu selama insiden.

1) Terapkan solusi EDR pada perangkat *endpoint* dan *server*
   a) *Tools* ini menjadi salah satu landasan tanggap insiden jika terjadi *ransomware* atau penyusupan/kompromi skala besar, memfasilitasi fase identifikasi, penahanan, dan remediasi.
   b) Lakukan EDR *search* dan *scanning* antivirus dengan menerapkan IoC untuk dapatkan indikator yang bermanfaat dalam melakukan perbaikan.
   c) Tetapkan kebijakan EDR dalam mode *prevention.*
2) Memblokir IoC yang terkait dengan aktivitas *malware* yang dikumpulkan oleh *threat intelligence.*
3) Menyebarkan dan mengoperasikan solusi keamanan yang memungkinkan deteksi dan memfasilitasi tanggap insiden
   a) Pengumpulan *log* dalam SIEM.
   b) Memiliki kapasitas untuk menjalankan *tools* seperti YARA atau DFIR-ORC (ANSSI) (https://github.com/dfir-orc).
4) Memiliki *log* dengan retensi dan verbositas yang baik.
5) Tentukan postur keamanan yang ketat dari sudut pandang penyerang.
6) Menyusun strategi komunikasi untuk pihak internal dan eksternal.
7) Memiliki proses setelah penyusupan/kompromi terdeteksi: reaksi secara diam-diam atau cepat.
8) Bersiaplah untuk memberi tahu lembaga penegak hukum serta regulator jika diperlukan selama insiden, sesuai dengan prosedur manajemen krisis.
9) Pada *endpoint*
   a) Diperlukan pengetahuan yang baik tentang kebijakan keamanan pada sistem operasi.
   b) Diperlukan pengetahuan yang baik tentang kebijakan profil pengguna *end user*.
   c) Pastikan bahwa *tools* pemantauan sudah *update*.
   d) Menjalin kontak dengan tim pengelola jaringan.
   e) Pastikan bahwa proses pemberitahuan *alert* ditetapkan dan diketahui semua pihak yang relevan.
   f) Pastikan semua peralatan mendapatkan *setting* pada NTP yang sama.
   g) Pilih jenis *file* apa yang bisa hilang/dicuri dan batasi akses untuk *file* rahasia.

h) Pastikan *tools* analisis aktif dan berfungsi, tidak disusupi, dan *update,* seperti antivirus, EDR, IDS, *log analyzer*.

10) Jaringan
    a) Pengetahuan yang baik tentang arsitektur, segmentasi VLAN, dan interkoneksi, sehingga memiliki kemampuan untuk mengisolasi entitas, wilayah, mitra bisnis, atau internet.
    b) Pastikan inventaris titik akses jaringan tersedia dan terbaru.
    c) Pastikan tim jaringan memiliki peta dan konfigurasi jaringan terkini.
    d) Cari titik akses jaringan potensial yang tidak diinginkan (xDSL, Wi-Fi, Modem, dan lainnya) secara teratur dan lakukan penutupan akses.
    e) Pastikan *tools* dan proses manajemen lalu lintas beroperasi.
    f) Diperlukan pengetahuan yang baik tentang aktivitas jaringan biasa dari aset informasi. Terdapat *file* di tempat aman yang menjelaskan aktivitas *port* biasa, untuk membandingkan secara efisien dengan keadaan saat ini.
11) Lalu lintas dasar (*baseline*)
    a) Mengidentifikasi lalu lintas dan arus yang mendasar (*baseline*) di jaringan.
    b) Mengidentifikasi proses bisnis yang bersifat kritis.

b. Identifikasi

Tujuan: mendeteksi insiden, menentukan ruang lingkupnya, dan melibatkan pihak yang tepat.

1) Perlu memberi tahu lembaga penegak hukum dan regulator di awal langkah ini jika diperlukan.
2) Deteksi
    a) Pemantauan IoC dari *thread intelligence* oleh SOC.
    b) Pengawasan *alert* dan *log* pada antivirus, EDR, SIEM, IDS.
    c) Terdapat *email* profesional yang aneh yang berisi lampiran.
    d) *Lateral movement* biasanya terjadi, periksa semua koneksi ke *server* AD dan ShareFile dengan akun istimewa pada hari yang tidak biasa.
    e) Banyaknya akun yang terkunci.
    f) Cari aktivitas penjelajahan jaringan atau *web* yang tidak biasa; terutama koneksi ke Tor I2P IP, Tor *gateway* (tor2web, dan lainnya) atau situs *web* pembayaran Bitcoin.
    g) Cari koneksi yang jarang.
3) Jika aset informasi teridentifikasi *malware*, maka cabut dari jaringan dan tetap hidupkan untuk penyelidikan forensik memori.
4) Lingkup kejadian

a) Gunakan EDR, *log* pada perangkat *endpoint*, *log* sistem, *tools* yang memungkinkan pencarian IoC dalam skala besar.
b) Mengidentifikasi teknik *pivoting* pada jaringan.
c) Meninjau statistik dan *log* perangkat jaringan.
d) Mengidentifikasi penggunaan berbahaya dari akun yang disusupi.
e) Mengidentifikasi *server* C2 di *log firewall*, *log proxy*, *log* IDS, *log* sistem, EDR, *log* DNS, NetFlow, dan *log router*.

5) Temukan vektor awal penyusupan/kompromi
   a) Menginvestigasi aset informasi yang terekspos, terutama yang tidak *up to date*.
   b) Verifikasi keberadaan *binary* di profil pengguna, %ALLUSERSPROFILE% atau %APPDATA% dan %SystemDrive%.
6) Catatan
   a) Identifikasi aktor ancaman pada asal serangan dapat membantu fase berikut berdasarkan TTP yang diketahui.
   b) Pada akhir langkah ini, aset informasi yang terkena dampak dan modus operandi serangan seharusnya telah diidentifikasi. Idealnya, sumber serangan juga harus diidentifikasi. Di sinilah harus dilakukan penyelidikan forensik. Amankan *backup* dan terputus dari ruang lingkup yang disusupi.

c. Penahanan (*Containment*)

Tujuan: mengurangi efek serangan terhadap lingkungan yang ditargetkan.

1) Jika masalah dianggap strategis karena mengakses sumber daya yang sensitif, maka jalankan prosedur manajemen krisis
   a) Pastikan bahwa semua sumber serangan telah diidentifikasi sebelum mengambil tindakan penahanan.
   b) Perjelas informasi dan data jika perlu dan memungkinkan.
2) Jika berlaku untuk serangan:
   a) Mengisolasi VLAN, interkoneksi, entitas, wilayah, mitra, atau internet yang disusupi
   b) Putuskan sambungan semua aset informasi yang terdeteksi telah disusupi dari jaringan. Isolasi perangkat dengan EDR dan mematikan internet, namun tetap mempertahankan koneksi EDR.
   c) Memblokir lalu lintas ke C2.
   d) Memblokir IP apa pun yang terdeteksi digunakan oleh penyerang.
   e) Nonaktifkan akun yang disusupi/dibuat oleh penyerang.
   f) Kirim sampel yang tidak terdeteksi ke penyedia keamanan *endpoint* dan/atau layanan *sandbox*.

g) Kirim URL berbahaya yang tidak dikategorikan, nama domain, dan IP ke penyedia keamanan perimetrik di organisasi.

3) Jika lalu lintas bisnis penting tidak dapat diputuskan, izinkan setelah memastikan bahwa jaringan tersebut bukanlah sumber infeksi atau temukan teknik penanganan yang tervalidasi.

4) Menetralkan vektor propagasi. Vektor propagasi dapat berupa apa saja mulai dari lalu lintas jaringan hingga cacat perangkat lunak. Penanggulangan yang relevan harus diterapkan, seperti *patch*, pemblokiran lalu lintas, penonaktifan perangkat, dan lainnya. Teknik berikut dapat digunakan:
   a) *Tools* penerapan *patch*, seperti Windows Server Update Services (WSUS).
   b) Windows GPO.
   c) Aturan *firewall*.
   d) DNS *sinkhole*.
   e) Hentikan layanan Sharefile.
   f) Hentikan koneksi atau proses yang tidak diperlukan pada aset informasi yang terpengaruh

5) Ulangi langkah 2 sampai 4 pada setiap sub area area yang terinfeksi sampai *worm* berhenti menyebar. Jika memungkinkan, pantau infeksi menggunakan *tools* analisis (*console* antivirus/EDR, *log server*, layanan *customer care* via telepon). Terapkan tindakan *ad hoc* jika terjadi masalah strategis:
   a) Blokir tujuan eksfiltrasi atau lokasi jauh pada filter internet.
   b) Batasi server *file* strategis untuk menolak koneksi dari komputer yang disusupi.
   c) Beri tahu pengguna bisnis yang ditargetkan tentang apa yang harus dilakukan dan apa yang dilarang.
   d) Mengonfigurasi kemampuan *logging* dalam mode *verbose* pada lingkungan yang ditargetkan dan menyimpannya di *server* yang aman secara jarak jauh.

d. Perbaikan (*Remediation*)

Tujuan: mengambil tindakan untuk menghilangkan ancaman dan menghindari insiden di masa depan.

1) Perangkat *endpoint*
   a) Menginisialisasi ulang semua akses ke akun yang terlibat dalam insiden tersebut.
   b) Hapus semua akun yang dibuat oleh penyerang.
   c) Hapus akses awal yang digunakan oleh penyerang.
   d) Hapus *binary* yang digunakan oleh penyerang untuk melakukan lateralisasi pada jaringan.
   e) Hapus persistensi.
   f) Ubah *password* pada akun yang disusupi.

g) Kembali ke perubahan konfigurasi.

h) Melakukan *hardening* pada sistem.

2) Jaringan

a) Temukan semua saluran komunikasi yang digunakan oleh penyerang dan blokir mereka di semua batas jaringan.

b) Jika sumber telah diidentifikasi sebagai orang dalam, maka ambil tindakan yang tepat, dan libatkan pihak manajemen, unit kerja SDM, unit kerja hukum.

c) Periksa apakah konfigurasi keamanan tidak tersentuh: *Group Policy Object* (GPO), antivirus, EDR, *patch*, dan lainnya.

d) Mengoperasikan *hardening* pada konfigurasi jaringan.

e) Jika penyerang telah diidentifikasi sebagai pelaku eksternal, pertimbangkan untuk melibatkan lembaga penegakan hukum dan regulator, jika diperlukan.

e. Pemulihan (*Recovery*)

Tujuan: memulihkan sistem ke operasi normal.

1) Prioritaskan rencana pemulihan berdasarkan *Disaster Recovery Plan* (DRP).

2) Semua langkah harus dilakukan secara bertahap dan dengan pemantauan teknis.

3) Perangkat *endpoint*

a) Pastikan bahwa tidak terdapat *binary* berbahaya di sistem sebelum menyambungkannya kembali.

b) *Best practice* adalah menginstal ulang sistem yang disusupi sepenuhnya dari media aslinya.

c) Terapkan semua perbaikan ke sistem yang baru diinstal.

d) Jika solusi ini tidak dapat diterapkan, maka lakukan hal berikut:

(1) Mengembalikan *file* yang diubah.

(2) Ubah semua *password* sesuai kebijakan *password* yang kuat.

4) Jaringan

a) Pastikan trafik jaringan sudah kembali normal dan aman.

b) Izinkan kembali lalu lintas jaringan yang digunakan sebagai metode propagasi oleh penyerang.

c) Sambungkan kembali sub-area jika perlu.

d) Sambungkan kembali area ke jaringan lokal jika perlu.

e) Sambungkan kembali area ke internet jika perlu.

5) Pantau lalu lintas jaringan untuk mengidentifikasi apakah masih ada infeksi. Jika memungkinkan, terapkan *geo-filtering* pada *firewall* untuk memblokir lalu lintas dari luar negeri yang tidak sah.

f. Pelajaran yang Diperoleh (*Lesson Learned*)

Tujuan: mendokumentasikan detail insiden, membahas pelajaran yang diperoleh, dan menyesuaikan rencana dan pertahanan teknis.

1) Laporan

   Laporan insiden harus ditulis dan tersedia untuk semua pihak yang relevan. Hal-hal berikut harus dijelaskan:

   a) Penyebab awal infeksi.
   b) Tindakan dan *timeline* setiap peristiwa penting.
   c) Apa yang sudah dilakukan dengan benar.
   d) Apa yang masih dilakukan dengan salah.
   e) Biaya insiden.
   f) *Indicator of Compromise* (IoC).

2) Catatan

   Tindakan untuk meningkatkan pertahanan *malware* dan proses deteksi intrusi jaringan harus ditentukan untuk memanfaatkan pengalaman ini, terutama *security awareness*.

Kosakata

***Endpoint Detection and Response* (EDR)** atau *Endpoint Detection and Threat Response* (EDTR) adalah solusi keamanan titik akhir yang terus memantau perangkat pengguna akhir untuk mendeteksi dan merespons ancaman siber seperti *ransomware* dan *malware*.

***Intrusion Detection System* (IDS)** adalah sistem yang memantau lalu lintas jaringan untuk aktivitas mencurigakan dan memberi peringatan (*alert*) saat aktivitas tersebut ditemukan.

***Intrusion Prevention System* (IPS)** adalah sistem keamanan jaringan yang terus memantau jaringan untuk aktivitas berbahaya dan mengambil tindakan untuk mencegahnya.

Konstituen Tim Tanggap Insiden Siber adalah pihak yang menerima manfaat dari layanan Tim Tanggap Insiden Siber.

Tim Tanggap Insiden Siber (*Computer Security Incident Response Team* - CSIRT) adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

Server C2 (command and control) adalah *server* yang digunakan penyerang untuk memelihara komunikasi dengan perangkat yang disusupi setelah eksploitasi awal. Mekanisme spesifik sangat bervariasi di antara serangan, tetapi C2 umumnya terdiri dari satu atau lebih saluran komunikasi rahasia antara perangkat di organisasi korban dan *platform* yang dikontrol penyerang.

Referensi

- Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon Software Engineering Institute: 2003.
- NIST Special Publication SP 800-61 rev.2 : Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology.
- Incident Response Methodology IRM #1 Malware Infection Response: Guidelines to handle information system Worm infections. Cert SG.
- Incident Response Methodology IRM #2 Windows Intrusion Detection: Live Analysis on a suspicious Windows system. Cert SG.
- Incident Response Methodology IRM #3 Unix/Linux Intrusion Detection: Live Analysis on a suspected system. Cert SG.
- Incident Response Methodology IRM #4 DDoS Incident Response: Guidelines to handle Distributed Denial of Service incidents. Cert SG.
- Incident Response Methodology IRM #5 Malicious Network Behaviour: Guidelines to handle a suspicious network activity. Cert SG.
- Incident Response Methodology IRM #6 Website Defacement: Live reaction on a compromised web server. Cert SG.
- Incident Response Methodology IRM #7 WINDOWS MALWARE DETECTION: Live Analysis on a suspicious computer. Cert SG.
- Incident Response Methodology IRM #8 Blackmail: Guidelines to handle blackmail attempt. Cert SG.
- Incident Response Methodology IRM #9 Malware On Smartphone: How to handle a suspicious smartphone. Cert SG.
- Incident Response Methodology IRM #10 Social Engineering Incident: How to handle a social engineering incident (phone or e-mail). Cert SG.
- Incident Response Methodology IRM #11 Information Leakage: Deal with internal information disclosed intentionally. Cert SG.
- Incident Response Methodology IRM #12 Insider Abuse: Guidelines to handle and respond to internal information disclosed intentionally. Cert SG.
- Incident Response Methodology IRM #13 Customer Phishing Incident Response: Guidelines to handle customer phishing incidents. Cert SG.
- Incident Response Methodology IRM #14 Scam Incident Response: Guidelines to handle fraudulent scam incidents. Cert SG.
- Incident Response Methodology IRM #15 Trademark Infringement Incident Response: Guidelines to handle and respond to trademark infringement incidents. Cert SG.

- Incident Response Methodology IRM #16 Phishing: Guidelines to handle and respond to phishing targeting collaborators. Cert SG.
- Incident Response Methodology IRM #17 Ransomware: Guidelines to handle and respond to ransomware infection. Cert SG.
- Incident Response Methodology IRM #18 Large Scale Compromise: Guidelines to handle and respond to large scale compromise. Cert SG.